January-February 2020
ISSN: 0193-4120 Page No. 8902 - 8907

Attack Localization Task Allocation Based Scheme for Implantable Medical Devices

Ms.A. Iyswariya, R.M.K. Engineering College
Mr.V.RamKumar, R.M.K. Engineering College
Ms.K.Jeevitha, R.M.K. Engineering College
Mr.V.Praveen Kumar, Nagman Instrumentation & Electronics Pvt. Ltd.

Article Info
Volume 82
Page Number: 8902 - 8907
Publication Issue:
January-February 2020

Article History
Article Received: *5 April 2019*
Revised: *18 Jun 2019*
Accepted: *24 October 2019*
Publication: *08 February 2020*

Abstract:
In this artificial intelligence dependent world, advantages and disadvantages of the technologies have equal foot. The transmission of data in medical field has a major drawback in security and privacy. Security plays a vital role in medical field as there can be adverse events. Implantable Medical Devices (IMD) is a man-made implantable device that helps in monitoring and treats the physiological conditions of human (temperature sensor for body temperature and pacemaker for heart beat rate). In our proposed system, we use IMD to monitor the conditions of the patient. In case of any abrupt changes in the monitored values, it records and sends the information to the controller node. This node collects the information and sends to the doctor through an access point. We can even send the data to the friends, relatives and trusted authority of patient's choice. Now by knowing the condition of the patient, doctor can prescribe the patient at right time even from a remote distance. This communication is allowed only after the two- wayverification between the user and the nodes by providing a secret session key. The security verification is done using Automaic Verification of Internet safety Pedantic and Applications tool (AVISPAT). This scheme provides safety to known attacks. Attack Localization Task Allocation (ALTA) is used to provide hash key to increase the safety. The practical demonstration is performed in NS2 simulation tool. Performance inspection of the intended scheme with living schemes is done with AWK graph.

Keywords: *Implantable Medical Devices (IMD), Controller node, mutual authentication, AVISPAT, ALTA, NS2 simulation, AWK graph.*

I. INTRODUCTION

Implantable Medical Device (IMDs) is a man-made device which monitors and treats the physiological conditions within the human body. Different types of IMDs are available they are brain neuro simulator, pacemaker, etc., ICT facilitates the communication between each devices by collecting and sending the data to nearby nodes using any of the communication technology A user (trusted authority like doctor etc.) can access the data from CN after a successful authentication.

However, in this technology developed an attacker can manipulate the weakness in the IMDs. The attacker can be a replay attacker, middle attacker or an impersonation attacker.

A secure user verification scheme has to be designed for IMDs to avoid these types of attacks.

The user and the IMD device establish session key in a secret manner and in addition verification is done by AVISPA tool which secure against the replay and man in the middle attack. The practical implementation is also done using NS2 simulations tool.

January-February 2020
ISSN: 0193-4120 Page No. 8902 - 8907

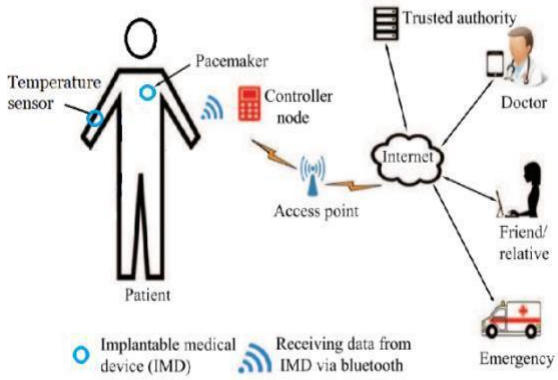

Fig. 1: Example of IMD

II. Proposed System

Remote authentication protocol which uses three factor namely smart card; password; biometrics is used for the, implantable medical gadget, that use elliptic curve algebraic structure over the finite fields.

ECC is applicable for many tasks like key agreement, pseudo-random generators and so on. Indirectly, they are used for the encryption. Elliptic curve consists of the points fullfillingp2 = q^3 + xq + y along the point at infinity. The point obtained from the curve intersection and straight-line R is given as addition of two definite points X and Y. Point multiplication can be computed through iterative addition which is an exponential approach. ECC is powerful.

Fuzzy extractor technique is used for biometric authentication that consists of following procedures namely: 1) producing secret biometric key of anchored size 2) Deterministic reproduction function Rep (.).

The network model presents the user with IMDs. These IMDs monitor health condition of patient and provides the service to the patient based on their symptoms. The patient is the user denoted as Ui. IMDs have wireless communication feature to transmit patient's information to the nearest node, say CNj, which collects the data securely. If the user needs the real-time information from CNj for monitoring and diagnosis, we require mutual authentication between the user *Ui* and the control node *CNj*, then the establish session key to each other for future communication with security.

Notation	Description
U_i, MD_i	i^{th} user and his/her mobile device
CN_j	j^{th} controller node
IMD_l	l^{th} implantable medical device
TA	Trusted authority
ID_i, PW_i, BIO_i	U_i's identity, password and biometric information
ID_{TA}, ID_{CN_j}	Identities of trusted authority and controller node
RID_i, RID_{CN_j}	Pseudo identities of U_i and CN_j
N	1024-bit secret number of TA
r_i, r_j	160-bit random nonces of U_i and CN_j
RTS_{CN_j}	Registration timestamp of CN_j
T_i	Generated current timestamp
ΔT	Maximum transmission delay associated with a message
$Gen(\cdot)$	Probabilistic generation procedure used in fuzzy extractor
$Rep(\cdot)$	Deterministic reproduction procedure used in fuzzy extractor
σ_i	Biometric secret key of U_i
τ_i	Public reproduction parameter of U_i
t	Error tolerance threshold used in fuzzy extractor
$E_p(a,b)$	A non-singular elliptic curve: $y^2 = x^3 + ax + b \pmod p$ over a prime finite field Z_p (Galois field $GF(p)$) with $a, b \in Z_p^*$ are constants with $4a^3 + 27b^2 \neq 0 \pmod p$
$k.P$	Elliptic curve point multiplication; $k \in Z_p^*$ & $P \in E_p(a,b)$
$h(\cdot)$	Collision-resistant cryptographic hash function
$\|, \oplus$	Concatenation and bitwise XOR operations

Table 1 : Notations used in paper

Random nonce and timestamps are used to protect from replay attack. The proposed scheme consists seven phases. They are

A.Pre-Deployment Stage

The authorized person is liable for node *CNj*and devices *IMDl* registration to their deployment in the deployment fields (Hospital). For the deployment, at first the trusted authority choose a distinctsafe number "N", for every*CNj* and along with it the

January-February 2020
ISSN: 0193-4120 Page No. 8902 - 8907

IMD'S attached in the body and then it calculates the pseudo identity for both the *CNj* and the IMDs. Finally it stores the information in the memory of *CNj* for deploying in the deployment field. To generate a pair wise key, a polynomial based protocol is used which is univariate.

Post-Deployment Phase: After the pre deployment phase, where once the IMD's and *CNj* are deployed, the first process in this phase is to establish a pair wise secret key. This is done with the help of prior information which is available in the memory. For the pair wise secret key to be established the *CNj* sends pseudo identity to IMD and then the IMD computes the shared key and hence it securely communicates.

B. User- Registration Phase

It deals with the registration procedure of the user *Ui*, to access information from the *CNj*. A trusted authority is required for registration. The doctor has to enroll at the Trusted authority which can be secure channel or the person. For registering, first the doctor determines an identity and direct to TA and after acquiring the acknowledgement, it delivers registration reply message to the doctor. Then the doctor selects a password of their choice and applies the biometric at the sensor to generate a biometric key.

C.Login Phase

For the login phase the doctor has to perform the following process. At first the doctor feeds ID and secured password to the mobile device (MD). The MD after comparing the hamming distance extracts the biometric key provided if the error is less than threshold value. If verification is correct then login takes place, else it is terminated.

D.Authentication Phase

In case, timeline matches controller node *CNj* computes and verifies the signature. After the computation controller node compute the session key and shared with user. After that *CNj* sends the authentication reply via public channel. After authentication reply, if it does not hold, user will suddenly cancel the connection. Then user checks if the condition holds *CNj*is authenticated by*Ui*. Then*Ui*will generate the timestampand send acknowledgement message through channel. After inheriting the information from the *Ui, CNj* will check the readiness. In case if the condition holds *CNj* will calculate. If it does not hold, then it will terminate the connection immediately or else the nodes collect the same key for safe communication.

E. Information Update Phase

Here password and biometric update facility is available in which, the user will able to change their password and biometric without involving TA for the security reason at any time. User will input their identity; password to their mobile devices also imprints their biometric information to the sensor *MDi.*User who canyon's theverification can make a start for upgrade procedure else the task will be suddenly terminated.

F.DynamicNode Addition Stage

The trusted authority will perform the Dynamic controller node addition. The trusted authority allocates a new special identity which is varied from the identities of existed controller node. Trusted authority will also compute polynomial share in GF.

G. Dynamic IMD Addition Phase

Another new Implantable Medical Devices is used to employ a new IMD to replace an existing IMD. The trusted authority will able to generate a different identity and calculate the similar pseudo identity and also the polynomial share. Them it will be stored in the memory of trusted authority. In controller node there will be no need to update the polynomial share. Only the trusted authority wants to inform the controller node about the deployment of implantable medical devices. It can determine the pair wise key with the controller node as *SKimd*. At last it starts secure communication using the determined key *SKimd* by the help of post deployment phase.

January-February 2020
ISSN: 0193-4120 Page No. 8902 - 8907

III. Security Analysis

The possible known attacks are shortly discussed below to which the intended system is safe.

A. Playback Attack

When a originator or an antagonist person repeats or delays the valid data transmission then the network attack is called replay or playback attack.Here, the messagesare exchanged between *Ui* and *CNj* with different timestamps in each phase. If anrival node obstructs these messages, the rationality of timestamps is failed and thus it provides protection by treating them as old messages.

B. Striker in the middle

Here the striker makes independent connection with the victims, who believe that they are communicating directly with each other. Authentication is the best way to prevent MITM. The attacker will not know the secret key; hence no modification can be done. Thus our scheme provides protection against MITM.

C. Userpastiche attack

Impersonation is a tool to gain access to the network for any fraud. Elliptic Curldistinct logarithm Problem is avoided in this method. Thus even if the attacker sends a valid login request to the control node, attacker do not know the secret biometric key, private key and correct password. Thus the security is maintained in this case too.

D. Controller Node pastiche Attack

If an attacker sends a valid authentication reply message to the user for the message sent during authentication and key establishment phase, due to ECDLP, attacker will never know the secret key.

E. Session Key Security

In one Session of communication all messages can be encrypted using a single use symmetric key called session key. One-way hash function protects all message session keys. Without knowing short-term secrets and long-term secrets, Attacker cannot compute session key SKij. Thus the proposed system provides security to sessions key.

F. Anonymity and Untraceability

If an attacker intercepts the informationduring login and verification stage, Due to acceptance of arbitrary nonce and current timestamps, secret key and private session key becomes changing and distinct for each session. It also does not directly include user and control node identification. Thus the intended system safeguards non-traceability prpoperties.

G. Resilience AgainstCN Physicalacquisition Attack

By physically acquiring a CN, with power analysis, attacker can get the required information. All pseudo controller node identity and pseudo personality RID are unique for controller nodes, and these are created by the Trusted Authority. Therefore, attacker can only find the session key but cant help in attacking the communication.

IV. Systematic Security Verification with AVISPA

A.Higher Level Protocol Specification Scheme

HLPSL is used as security protocol. The translator HLPSL2IF converts HLPSL into the intermediate format (IF) and read directly by AVISPA tool.

The output format is produced by back end which indicates the safety of the protocol. For unsafe condition it gives list of attack trace. The intendedsystem is simulated using the Security pedantic animator for AVISPA.

B.Attack Localization Task Allocation

In our Attack Localization Task Allocation techniques we implemented the SHA512 hash key techniques. In these SHA512 is better than SHA 1 and latest SHA 256. The length of the key is increases the security also increases. compression functions. The secure hashing algorithm creates constant length string. SHA-1, SHA-2, and SHA-5, are created with stronger encryption to hacker attacks. Secure ashing algorithm is used to encrypt

January-February 2020
ISSN: 0193-4120 Page No. 8902 - 8907

passwords so that server tracks only the user's hash value. If the hacker attacks the data base , hacker can find only the hash value. Additionally, SHA exhibit the avalanche effect. Tampering can also be detected using SHA.

V. Practical Perspective:NS2 Simulation Study

NS (version 2) is an network simulator written in C++ and OTcl. NS is for simulating LAN and WAN. The following parameters are used in stimulation

- No of Nodes: 11
- Frequency: 50Hz
- Routing Protocol: DSDV
- Antenna: Omni Antenna
- Channel: Wireless Channel

The pattern of data transmission in WIFI network is viewed in the NS2 stimulator. The algorithm used for this is as follows

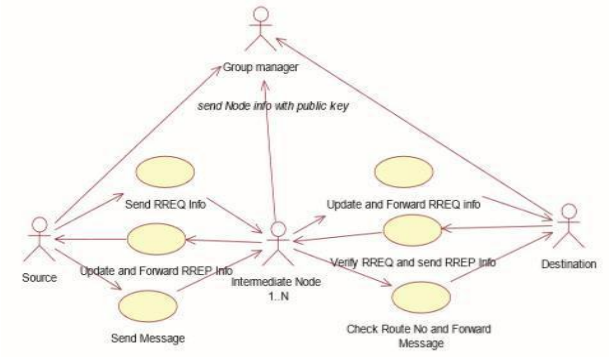

Fig.2: Algorithm for data transmission

VI. Result

Some performance parameters are calculated and stored in the database as trace in hexadecimal form to measure the impacts of this scheme. These data help in graph formation using AWK language. The parameters included are end-to-end delay, loss, throughput, channel frequency, drop node frequency, source frequency, destination frequency and protocol frequency.

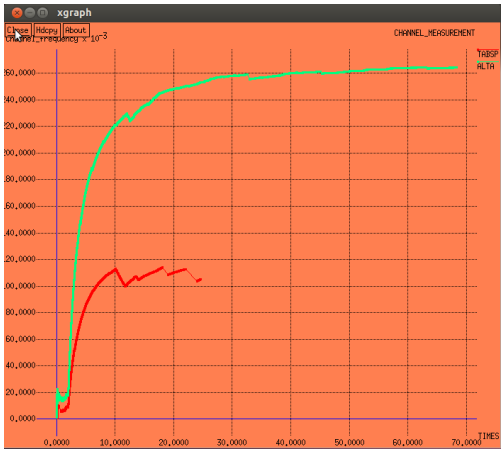

Fig.3: Channel Frequency versus time

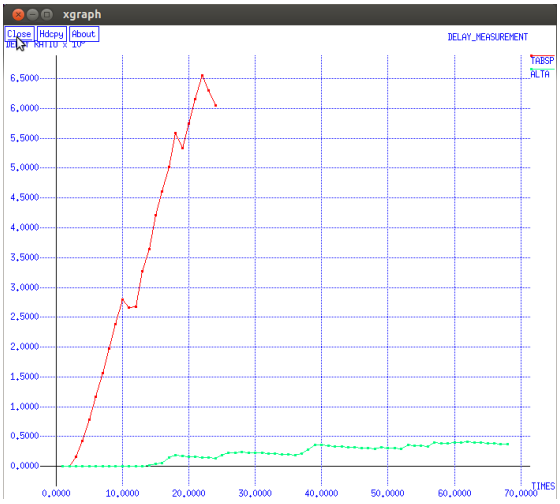

Fig.4 : Delay versus Time

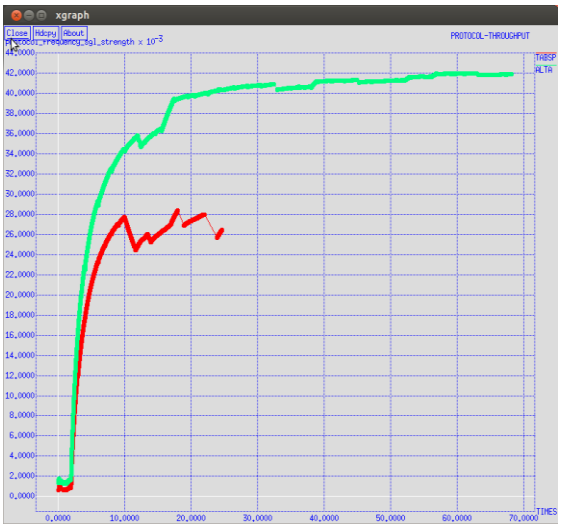

Fig.5: Protocol signal frequency strength versus time

January-February 2020
ISSN: 0193-4120 Page No. 8902 - 8907

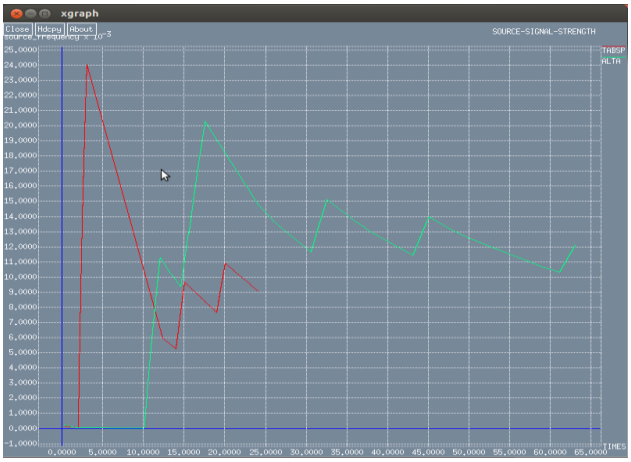

Fig.6: Source frequency versus time

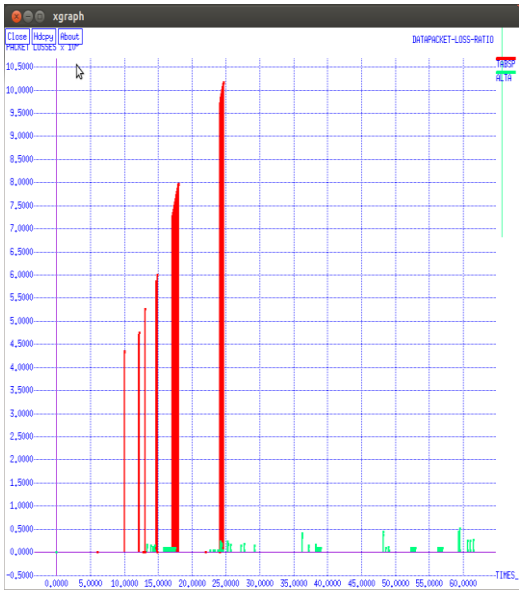

Fig.7 : Packet loss versus time

VII. Conclusion

In this paper, ALTA technique scheme is used to improve the communications having the hash key value for each data as followed by SHA1. The IMD treats and monitors a physiological condition of human body and also helps the doctor in remote consultation. Secure communication can be established using a session key mutually authenticated by control node and the doctor. Additionally, a comparative graph has been produced between exciting and proposed scheme which has a high level security base.

VIII. References

[1] X. Li, J. Niu, S. Kumari, F. Wu, and K. K. R. Choo, "A robust biometrics based three-factor authentication scheme for Global Mobility Networks in smart city," Future Generation Computer Systems, 2017, DOI: 10.1016/j.future.2017.04.01

[2] D. He and S. Zeadally, "An Analysis of RFID Authentication Schemes for Internet of Things in Healthcare Environment Using Elliptic Curve Cryptography," IEEE Internet of Things Journal, vol. 2, no. 1, pp. 72– 83, 2015.

[3] M. Rushanan, A. D. Rubin, D. F. Kune, and C. M. Swanson, "SoK: Security and Privacy in Implantable Medical Devices and Body Area Networks," in IEEE Symposium on Security and Privacy, San Jose, USA, 2014, pp. 524–539.

[4] D. He, N. Kumar, J. H. Lee, and R. S. Sherratt, "Enhanced threefactor security protocol for consumer USB mass storage devices," IEEE Transactions on Consumer Electronics, vol. 60, no. 1, pp. 30–37, 2014.

[5] N. Ellouze, M. Allouche, H. Ben Ahmed, S. Rekhis, and N. Boudriga, "Securing Implantable Cardiac Medical Devices: Use of Radio Frequency Energy Harvesting," in Proceedings of the 3rd International Workshop on Trustworthy Embedded Devices, Berlin, Germany, 2013, pp. 35–42