IF : 3.62 | IC Value 80.26

Volume-5, Issue-12, December - 2016 • ISSN No 2277 - 8160

Original Research Paper

Medical Science

Secure Data Transmission in Wireless Body Area sensor Network

S.Karthik Mphil Research Scholar, Muthayammal College of Arts & Science, Rasipuram

L.Devi Assistant Professor, Muthayammal College of Arts & Science, Rasipuram

S.Bharathi Assistant Professor, Muthayammal College of Arts & Science, Rasipuram

ABSTRACT

Medical health care system improved with new innovation and techniques, reducing the time, easy to monitoring the patients via the wireless body area sensor network. In the online healthcare industry new technologies are implemented. Today security in Wireless sensor network is very mitigating. Researchers challenge is developing security in the sensor nodes. Many researchers develop the secure transmission techniques here the existing method is Ecliptic curve cryptography; it is developed for time-consuming and power consuming. This technique is implemented in the body area sensor network. The ECC Elliptic curve cryptography system is the key distribution method. The proposed method describe the selection of node and it filter the false data improve the security level using the time efficient sink detection algorithm. The proposed method includes the how the packets are forwarded and securely transmitted and drop out the false data. These methods are implemented in the body area sensor network.

KEYWORDS : ECC, Time efficient algorithm, drop out data.

Introduction:

Wireless body area sensor network is portability and unobtrusive-ness. Small devices collect data and communicate wirelessly, operating with minimal patient input. They may be carried on the body or deeply embedded in the environment. Unobtrusiveness helps with patient acceptance and minimizes confounding measurement effects. Since monitoring is done in the living space, the patient travels less often, which is safer and more convenient. Ease of deployment and scalability Devices can be deployed in potentially large quantities with dramatically less complexity and cost compared to wired networks. Devices are placed in the living space and turned on, self-organizing and calibrating automatically. Real-time and always-on . Physiological and environmental data can be monitored continuously, allowing real-time response by emergency or healthcare workers. The data collected and are sending to the data server for filling in the traditional patient history. Even though the network as a whole is always-on, individual sensors still must conserve energy through smart power management and on-demand activation.

SYSTEM ARCHITECTURE

System overview

Heterogeneous devices are integrated in the wireless sensor network system. Some devices are wearable on the patient and some placed inside the living space. Devices are inform the patient data collectively, aggregately, and stored in the memory chip also.

The healthcare provider networks are connecting the server system by gateway or directly connect to the medical server. Bluetooth and the GPS technologies are introduced. The three tier architecture are shown in Figure 1, each tier of the architecture is described below.

Body Network and Subsystems

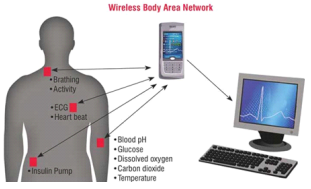

Figure 1: Wireless Body Area Network Architecture

This network comprises tiny portable devices equipped with a variety of sensors (such as heart-rate, heart-rhythm, temperature, oximeter, accelerometer), and performs biophysical monitoring, patient identification, location detection, and other desired tasks. These devices are small enough to be worn comfortably for a long time. Their energy consumption should also be optimized so that the battery is not required to be changed regularly.

Existing method

Elliptic Curve Cryptography (ECC)

Elliptic Curve Cryptography (ECC) was discovered in 1985 by Victor Miller (IBM) and Neil Koblitz (University of Washington) as an alternative mechanism for implementing public-key cryptography. Public-key algorithms create a mechanism for sharing keys among large numbers of participants or entities in a complex information system. Unlike other popular algorithms such as RSA, ECC is based on discrete logarithms that are much more difficult to challenge at equivalent key lengths.

At the time of its discovery, the ECC algorithm was described and placed in the public domain. What others found was that while it offered greater potential security it was slow. Certicom focused its efforts on creating better implementations of the algorithm to improve its performance. After many years of research, Certicom introduced the first commercial toolkit to support ECC and make it practical for use in a variety of applications.

Other cryptographers have also become interested in ECC. Today Certicom sponsors the Centre for Advanced Cryptographic Research (CACR) at the University of Waterloo, Ontario along with the Canadian government, Mondex, MasterCard International, and Pitney Bowes. Each year the Centre sponsors an ECC workshop attended by over 100 top cryptographers to discuss advances in the field of elliptic curve cryptography.

Other important industry activity is bringing additional credibility to the technology. The Certicom ECC Challenge offers an opportunity for people around the world to create new methods of attacking the algorithm and exposing any weaknesses. The longer an algorithm stands up to attack the more confidence developers have in its ultimate security. The ECC Challenge started in November

1997 and still runs today. Certicom hosts an annual Certicom ECC Conference, which brings together thought leaders, researchers and industry executives to talk about ECC and its applications.

Also important is the formation of the Standards for Efficient Cryptography Group. The SECG is a consortium of leading providers of cryptography and information security solutions who have united to address the lack of interoperability between today's different cryptographic solutions.

Proposed Method

Group based collaborative neighbor selection time efficient sink detection algorithm

TSD provides the sink node to either obtain the event or discard the event, if it is considered to be false data. Sensor nodes in Wireless Sensor Network broadcast the packets to the destination nodes through the sink nodes. If the destination node is nearer, the sensor nodes directly transfers or broadcasts the packets to it without the support of any other neighboring nodes. On the other hand, if the distance between the source node and destination node are higher, then it has to be broadcasted through neighboring sensor nodes which it turn sends the packets to the sink node.

Efficient packet forwarding through router nodes via TSD is formalized as given below

$$PF_i = R_1 \cup R_2 \cup R_3 \ldots\ldots \cup R_n$$

In this way bandwidth efficiency is maintained using Group based Collaborative Neighbor Selection mechanism. Moreover, the data aggregated and forwarded packets are secured through Time-efficient Sink Detection algorithm.

Algorithm – Time-efficient Sink Detection

Step 1: Detection of an event '*E*' by group source nodes $S_1, S_2, \ldots, S_n$ with time of occurrence of event 'T' with time for each node set as 'τ'
Step 2: Select the neighbor nodes '$N_1, N_2, \ldots, N_n$'
Step 3: Send the detected event '(E, P, T)', with router information '$R_1, R_2, \ldots, R_n$'
Step 4: if source nodes consider event E as true and $\tau < T$
Step 5: $SD = (E, P)$
Step 6: else
Step 7: *SD* discard the event '*E*'
Step 8: end if
Step 8: Check the existence of $N_i(E_i, P_i)$
Step 9: if $(E_i, 1 \leq i \leq N_i)$ then consider the packet to be secured, else
Step 10: Discard the packet other wise
Step 11: end if
Step 12: end
Output Secured data aggregated and forwarded packets

Objective of study

- Supporting healthcare applications are in easily development stage, it is a valuable contributions at monitoring diagnostic or therapeutic levels
- Secure data communication and low power consumption.
- Reduce false data with new techniques.

Conclusion and Future work

During the packet transmission in wireless body area sensor network to improving the security by neighbor node selection method using of the time efficient sink detection algorithms.

Filtering the positive data is mitigating for every sensor node so implementing of the TSD the time efficient is calculated and the rate are measured by the simulator tools. Security also improved and neighbor selection is made very securely. To improve selection in efficiently time updating algorithms are implemented with star topological method is our future work.

References:

1. Dr M.Gobi and D.Kannan A Secured Public Key Cryptosystem for Biometric Encryption International Journal of Computer Science and Information Technologies, Vol. 5 (1) , 2014, 184-191.
2. Shashi Kant Shankar, Anurag Singh Tomar,Gaurav Kumar Tak* Secure Medical Data Transmission by using ECC with Mutual Authentication in WSNs,4th international conference on Eco- friendly computing and communication System. Science Direct.ICECCS 2015.
3. Samaneh Movassaghi, Mahyr Shirvanimoghaddam, Mehran Abolhasan, David Smith. An energy efficient network coding approach for wireless body area networks. IEEE; 2013.
4. FirozehEskandari and Mehdi Javanmard," Combining Filtering Techniquesin Wireless Sensor Network", Advances in Natural and Applied Sciences", AENSI Journals,Sep 2014.
5. Crisotto "an implementation of a wireless body area network for Ambulatory health monitoring"The University of Alabama in Huntsville , 2006
6. Anuja Aroraa, Apoorva Khera ,"Wi-Fi Enabled Personal Computer Network Monitoring System Using Smart Phone With Enhanced Security Measures" ScienceDirect *4thInternational Conference on Eco-friendly Computing and Communication Systems Available online at www.sciencedirect.com.