Biomedical Research 2018; 29 (20): 3708-3714

ISSN 0970-938X
www.biomedres.info

IOT based monitoring system to detect the ECG of soldiers using GPS and GPRS.

Anuradha M[1*], Sheryl Oliver A[1], Jean Justus J[1], Maheswari N[2]

[1]St. Joseph's College of Engineering, Chennai, Tamil Nadu, India

[2]VIT University, Chennai, India

Abstract

Technology has derived greater value and integrity since the conception of biometric systems. The idea of enhancing security through biometric authentication is proved greatly successful and gained widespread approval because every human being has a unique signature that cannot be replicated. Fingerprints and retinal scans are commonly used biometric authentication techniques. In recent years, facial recognition is also a preferred method of digital authentication. However, in this paper, a system to recognise clinical electrocardiogram (ECG) as a biometric feature for soldiers to communicate in the designated radio frequency has been proposed. The system proposed is a walkie-talkie that uses a wireless sensor network with IOT based monitoring system to detect the ECG of soldiers. The ECG of human beings like their fingerprints and retina are unique and cannot be misused after the respective person was dead. The main purpose of this Walkie-Talkie is to secure the communication medium used by armed forces during warfare and to alert the troops in case of an emergency. Its operations are based on the soldier's pulse rate. The Walkie-Talkie also has an inbuilt global positioning system (GPS), to identify the location of the soldier during active battle by using the longitude and latitude values. If the pulse is normal, the connection will be established between the control station and the walkie-talkie. Else, the walkie-talkie will be disconnected within three minutes based on relay settings monitored by the control station. The control station will receive an update message from the soldier's walkie-talkie every two minutes and an alert will be sent to the head of the battalion in critical situations. Technology has derived greater value and integrity since the conception of biometric systems. The idea of enhancing security through biometric authentication is proved greatly successful and gained widespread approval because every human being has a unique signature that cannot be replicated. Fingerprints and retinal scans are commonly used biometric authentication techniques. In recent years, facial recognition is also a preferred method of digital authentication. However, in this paper, a system to recognise clinical electrocardiogram (ECG) as a biometric feature for soldiers to communicate in the designated radio frequency has been proposed. The system proposed is a walkie-talkie that uses a wireless sensor network with IOT based monitoring system to detect the ECG of soldiers. The ECG of human beings like their fingerprints and retina are unique and cannot be misused after the respective person was dead. The main purpose of this Walkie-Talkie is to secure the communication medium used by armed forces during warfare and to alert the troops in case of an emergency. Its operations are based on the soldier's pulse rate. The walkie-talkie also has an inbuilt global positioning system (GPS), to identify the location of the soldier during active battle by using the longitude and latitude values. If the pulse is normal, the connection will be established between the control station and the walkie-talkie. Else, the walkie-talkie will be disconnected within three minutes based on relay settings monitored by the control station. The control station will receive an update message from the soldier's walkie-talkie every two minutes and an alert will be sent to the head of the battalion in critical situations.

Keywords: Global positioning system (GPS), General packet radio services (GPRS), Electrocardiogram (ECG), Walkie-talkie.

Accepted on November 19, 2018

Introduction

The main aim of this system is to ensure secure communication between soldiers and the control station in the battlefield. The use of biometrics for authentication is becoming more and more mainstream [1]. Nowadays, various devices come fitted with fingerprint [2] or iris scanners used for identity verification. Another biometric feature [3-5], which is unique

to every individual, is the heartbeat which can be measured with an electrocardiogram (ECG) [6-18]. Compared to other features, the human heartbeat is hard to falsify, since it naturally holds information about whether an individual is alive or dead. One disadvantage, when compared with other biometric features is the time needed for data acquisition. There are several physiological reasons why heartbeat differs with every human [19]. The first reason is the structure of the human heart which is unique to every person. The electrical conductivity of the cardiovascular cells, as well as muscle fibre orientation and the Purkinje System, are some major reasons why heartbeats differ for each individual. Apart from this, the location of the heart is also another cause for differences in the ECG patterns. Sex, age, height and the body habitus also play a role [20]. There are various approaches for isolating these differences. One approach involved identifying fiducial points [21] in a segmented heartbeat. Based on these fiducial points, differences in amplitude and time, as well as angles between those points can be computed which are believed to be unique for every individual and can, therefore be used as a feature for classification.

The idea is to disconnect the communication between the soldier's wireless device and control station if he gets killed in battle or if the device was removed from the soldier without the knowledge of the control station in order to prevent sensitive data from falling into the wrong hands. Also, to send am alert to the crew head in case of crisis. The control station receives a message from the soldier's walkie-talkie (using the GPRS) every two minutes. This message contains the pulse condition (normal or abnormal) of the soldier and the latitude and longitude values of the soldier's position. By analysing this message the control station decides whether to establish a connection to that soldier. If the soldier is attacked, then the connection gets severed. Then, the control station contacts the nearest soldier to provide help. Thus, providing a secure wireless communication in the military war field.

Existing System

Wireless communication [23] devices are most widely used nowadays. Their use has grown much in residential and military sectors. Walkie-talkie [22] are used in the military for communication purpose among the soldiers, especially on their battlefield. Walkie-talkie is half-duplex devices which are used to communicate with soldiers to report their current status to the base and also to receive orders back from the base. It is very easy to handle which might become a problem if the device falls into the wrong hands. There is no possible way to find who is using the device. Anybody can get their hands on it and thus there is a high chance of the vital intelligence getting leaked.

Motorola GP338 plus

One of the existing systems of the walkie-talkie used in the military is the Motorola's GP338 plus walkie-talkie (Figure 1). The GP338 Plus offers a versatile two-way solution for professionals who need to stay in contact and require additional features. This practical radio can easily increase productivity by keeping soldiers communicating, yet streamlines their radio use-allowing them to concentrate on the job at hand. The GP338 Plus provides a maximum of 128 channels, an easy to read on-screen LCD display and uses MDC 1200 signalling.

Figure 1. *Motorola GP338 plus.*

Talk pro H350 plus

H350 plus multi-function super value is another professional walkie-talkie for Army, Railways, Ports, Cement and Steel industries, Coal mines, Thermal Plants and Infrastructure manufactured by Talk Pro (Figure 2).

Figure 2. *Talk pro H350 plus.*

H350 plus walkie-talkie provides a maximum of 16 channels, with MDC 1200 signalling and IP67 MIL Standards. It also allows emergency transmit to all radios, wire clone and has a 5-tone signalling and siren.

Proposed Architecture

In the proposed system (SCF48) to overcome the disadvantages of the existing systems and to improve secure communication between the soldier and the control station is

embedded a heartbeat sensor in the soldier's walkie-talkie (which ensures the soldier is an authorized person by recognising their heartbeat), together with a GPS (to track the location of the soldier) [24-27] and a GPRS (to send the soldier's status to the control station every two minutes) (Figure 3) [28].

This safeguards the communication between the soldier and the control station in the battlefield, by disconnecting the communication whenever the soldier's heartbeat status falls abnormally.

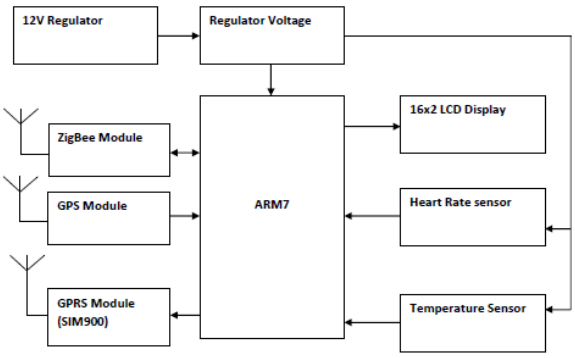

Figure 3. *Architecture diagram of the proposed system.*

The proposed architecture consists of four main modules. The heart rate sensor, GPS module, microcontroller and the GSM/GPRS module. The heart rate sensor monitors the soldier's heartbeat rhythm as well as calculates the heart rate of the soldier and sends it as an external interrupt to the microcontroller. At the same time, the GPS locates the soldier's position and despatches the latitude and longitude values to the microcontroller *via* the UART port through which it is attached peripherally to the microcontroller.

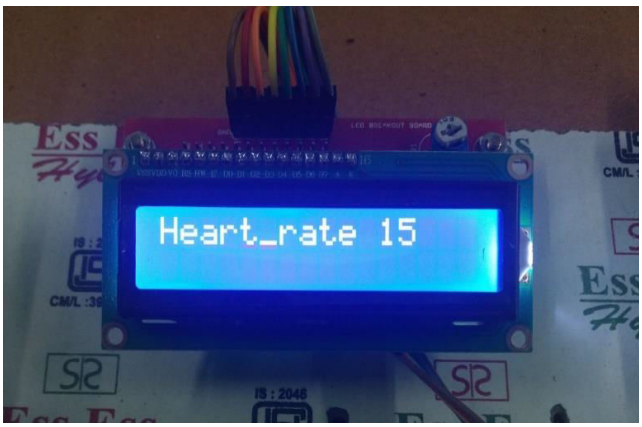

Figure 4. *Measuring soldier's heart rate.*

Then, the microcontroller executes a comparison between the heartbeat rhythm of the soldier monitored by the heart rate sensor and the heartbeat rhythm of the soldier stored as a digital file in it, also checks if the heart rate of the soldier is normal or not. Once the comparison is done it sends the status of the soldier as normal (when the soldier's heartbeat rhythm monitored by the heart rate sensor matches with the digital file stored in the microcontroller and the heart rate is normal) or abnormal (when the heartbeat rhythm doesn't match and the heart rate is not normal) along with the soldier's current latitude and longitude to the GSM/GPRS *via* the UART port by means of which it is peripherally connected to GSM/GPRS. The GSM/GPRS module then updates the control station server with this message every two minutes. The same process is repeated over and over.

As long as the status of the soldier is normal the control station continues to transmit messages to the soldier. Suppose, when the soldier's status is abnormal the control station immediately terminates the communication between the soldier and contacts another soldier who is nearest to that soldier to check on him.

Implementation

Heart rate sensor

The human heart beats at a unique rate for each individual. No two heart rates can be same [19]. The heart rate sensor exploits this concept in sensing the heart rates of soldiers in military camp. The heart rates of each soldier are discretely recorded as a digital file, stored in the database.

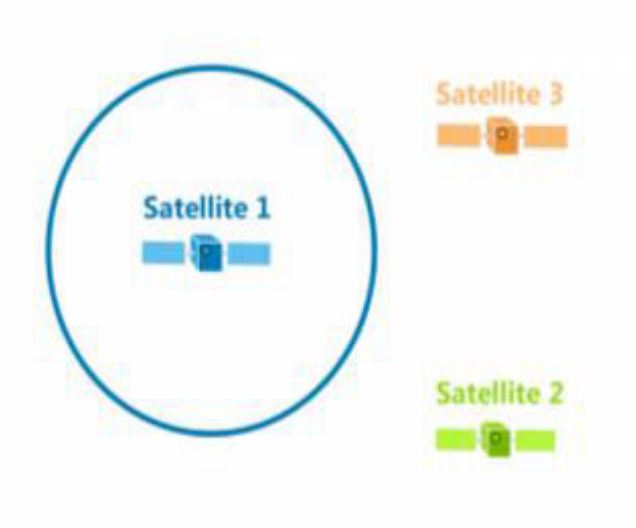

Figure 5. *Data from single satellite.*

The walkie-talkie [22] is modified by including the above-mentioned sensor. This sensor measures the heartbeat of the soldier and the result is compared with the digital file in the microcontroller which is also included in the walkie-talkie design (Figure 4).

GPS module

The GPS (Global positioning system) [24-27] module is a peripheral device connected to the microcontroller *via* the UART (Universal Asynchronous Receiver Transmitter). The GPS module continuously tracks the location of the soldier using the trilateration method and sends the location coordinates to the microcontroller. The microcontroller then sends the location coordinates of the soldier to the GPRS module which sends the data to the server.

Trilateration

Trilateration is a sophisticated version of triangulation. Data from a single satellite pinpoints a position to a large area of the earth's surface (Figure 5). Adding data from a second satellite narrows the position down to the region where the two spheres of satellite data overlap (Figure 6). Further, adding data from a third satellite provides a relatively accurate position, and all the GPS units require more than four satellites-enhances precision and determines accurate elevation or altitude (Figure 7).

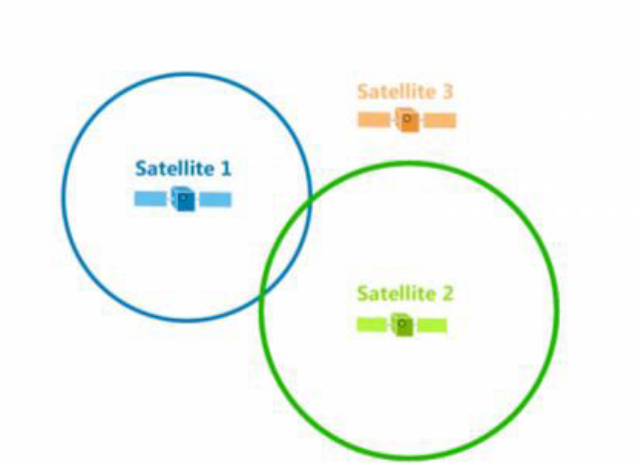

Figure 6. *Data from two satellites.*

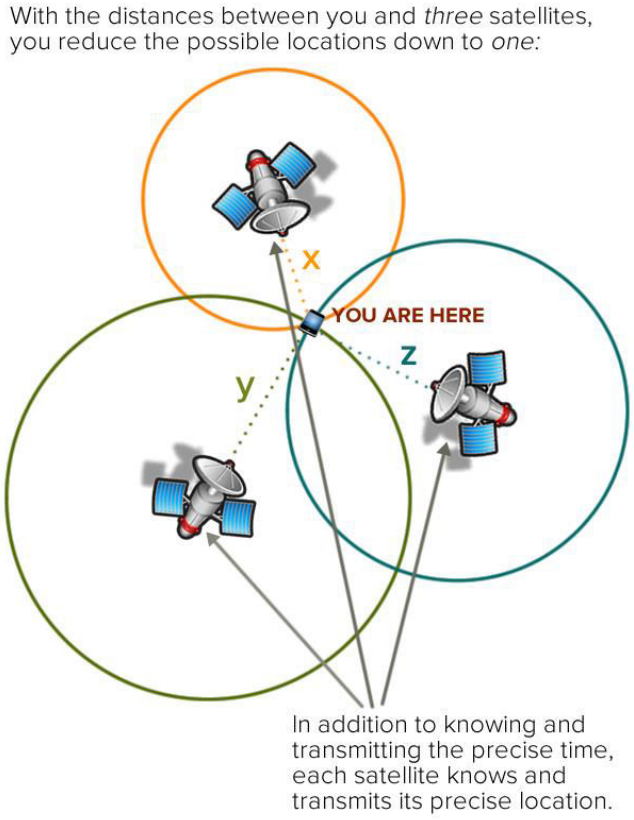

Figure 7. *Trilateration in GPS.*

GPS receivers routinely track four to seven satellites or even more simultaneously and use trilateration to analyse the information.

The GPS calculation in the receiver uses four Equations 1-4, in the four unknowns *x, y, z,* t_c. The four equations are,

$$d_1 = c(t_{t,1} - t_{r,1} + t_c) =$$

$$\sqrt{(x_1 - x)^2 + (y_1 - y)^2 + \sqrt{(z_1 - z)^2}} \rightarrow (1)$$

$$d_2 = c(t_{t,2} - t_{r,2} + t_c) =$$

$$\sqrt{(x_2 - x)^2 + (y_2 - y)^2 + \sqrt{(z_2 - z)^2}} \rightarrow (2)$$

$$d_3 = c(t_{t,3} - t_{r,3} + t_c) =$$

$$\sqrt{(x_3 - x)^2 + (y_3 - y)^2 + \sqrt{(z_3 - z)^2}} \rightarrow (3)$$

$$d_4 = c(t_{t,4} - t_{r,4} + t_c) =$$

$$\sqrt{(x_4 - x)^2 + (y_4 - y)^2 + \sqrt{(z_4 - z)^2}} \rightarrow (4)$$

Where,

x, y, z=receiver's coordinates

tc=time correlation for the GPS

c=speed of light (3 × 108 m/s)

$t_{t,1}$, $t_{t,2}$, $t_{t,3}$, $t_{t,4}$=times that GPS satellites 1, 2, 3 and 4, respectively, transmitted their signals

$t_{r,1}$, $t_{r,2}$, $t_{r,3}$, $t_{r,4}$=times that GPS satellites 1, 2, 3 and 4, respectively, are received

x_1, y_1, z_1=coordinates of GPS satellite 1; similarly, for x_2, y_2, z_2, etc.

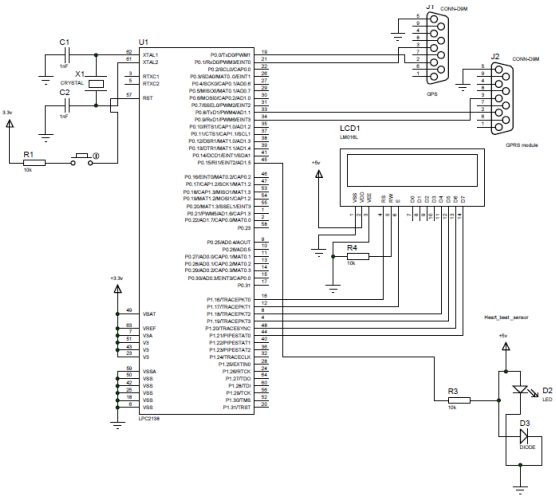

Figure 8. *Circuit diagram of LPC2148 interfacing with GPS, GSM/ GPRS, heart rate sensor and LCD display.*

ARM7 LPC2148

The ARM LPC2148 microcontroller interfaced with the GPS, GSM/GPRS module and the heart sensor is embedded in the soldier's walkie-talkie. The GPS continuously tracks the location of the soldier and transmits the longitudinal and latitudinal values to the microcontroller (Figure 8). Meanwhile, the heart rate sensor monitors soldier's heartbeat and sends the soldier's heart rate status data to the microcontroller.

The microcontroller then broadcasts the data it received from the GPS and heart rate sensor to the GSM/GPRS module interfaced with it. The GSM/GPRS module then forwards the data to the server which can be accessed by the control station. The GSM/GPRS persists to send the data to the server every two minutes until the communication between the soldier and the control station lasts. The microcontroller also sends an alert to the troop head when the soldier's heart rate status is abnormal which tells that the soldier is in danger.

GSM/GPRS module

GSM/GPRS module comprising of a GSM/GPRS modem with standard communication interfaces like RS-232 (serial port), USB, etc., a slot for inserting SIM (Subscriber identity module) and a power supply circuit is interfaced with the ARM7 LPC2148 microcontroller *via* the UART (Universal asynchronous receiver transmitter) port.

The GSM/GPRS module keeps the control station updated by sending the data (soldier's Heart rate status and current location coordinates) to the server every two minutes. Based on the message from the GSM/GPRS [28] module communication is set up between the soldier's walkie-talkie and the control station (Figure 9).

Algorithm

Let Get_Details () be a function which returns the latitude and longitude values (using GPS) and Heart rate status of the soldier (using Heart rate sensor) from the microcontroller.

While (Connection exists)

Get_details ();

Establish a connection with the remote server having static IP;

Send data packets to the server;

End while

Steps:

1. The GPRS module in the soldier's walkie-talkie updates the server with the latitude and longitude values of the soldier's position and the heart rate status of the soldier.

2. The control station checks the server for updates periodically.

3. From the updates, the control station decides based on the soldier's heart rate status.

4. If the soldier's heart rate status is normal the control station transmits the messages.

5. Suppose, if the soldier's heart rate is not normal then the control station terminates the connection to that soldier and sends another nearest soldier for help.

6. Again the same process is repeated from step 1 through step 5.

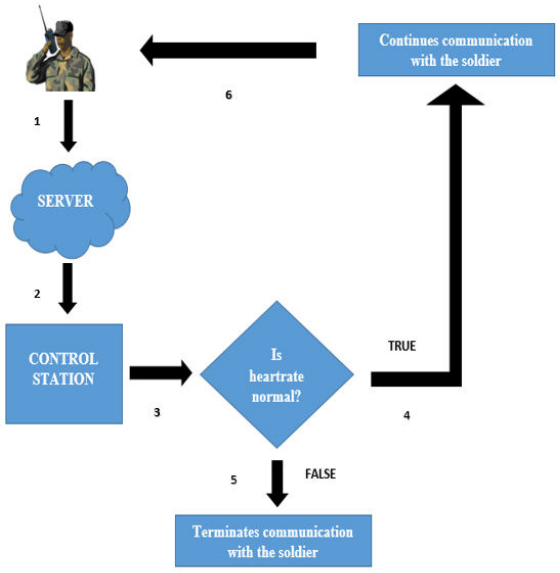

Figure 9. *Flowchart of the GSM/GPRS module implementation.*

Performance Analysis

Location accuracy

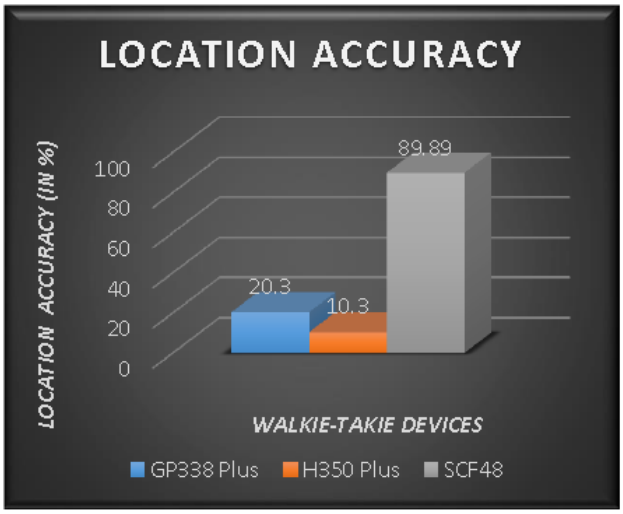

Figure 10. *Comparison of location accuracy between the existing systems-(GP338 plus and H350 plus) and the proposed system (SCF48).*

In Figure 10, the performance measure of the proposed system and the existing system (Motorola GP338 Plus and Talk Pro H350 Plus) are compared in terms of location accuracy. Location accuracy can be defined as how precise one's location

is. Location accuracy is much more important in the battlefront.

The graph clearly, shows that the proposed system has higher location accuracy than Motorola GP338 Plus and Talk Pro H350 Plus, as it has GPS embedded in it.

Thus, in the existing systems-the location accuracy was 20.3% in GP338 Plus and 10.3% in H350 Plus whereas in the proposed system the accuracy is increased to 89.89%.

Confidentiality

Another factor to be considered is confidentiality. Here, confidentiality refers to how secret is the delivered message.

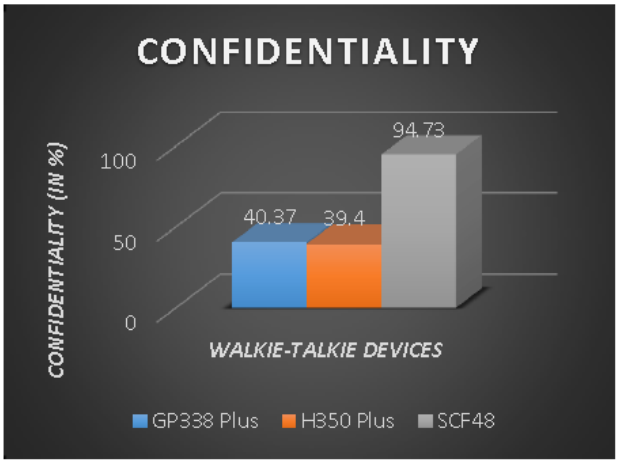

Figure 11. *Comparison of confidentiality between the existing systems-(GP338 Plus and H350 Plus) and the proposed system (SCF48).*

Taking this fact into consideration, the existing systems (Motorola GP338 Plus and Talk Pro H350 Plus) are less confidential compared to the proposed system. As the proposed system uses the soldier's heart rate as biometric authentication, the proposed system is much more reliable in maintaining the confidentiality of the message transmitted during the war in the battlefield compared to the existing system. This can be inferred from the following graph that the confidentiality in the existing system is 94.73% wherein the existing system it is 40.37% in GP338 plus and is 39.4% in H350 plus (Figure 11).

Conclusion

The modified walkie-talkie using GPS, GPRS and heart rate sensor on implementation hopes that the experimental results will result in the increased concealment among the messages transmitted between the soldiers and the control station during the warfare. In the case when the enemy outbreaks the soldier, he can't receive the message broadcasted to the soldier from the control station, as the device is authenticated with the soldier's heartbeat and the connection between the soldier and the base is terminated and an alert is sent to the crew head when the soldier's heart rate status is abnormal. Also, the base station sends the nearby soldier to help the attacked soldier, using the location provided by GPS in the soldier's device.

Therefore, this device is much more efficient and secure than the previously developed devices. They provide high security and ensure the distribution of vibrant data. Subsequently, this device is provided with GPS, the location of the soldiers is sent periodically to the base and the server is updated regularly. Thus, this model is anticipated to have great use in the military war field in the upcoming years.

Future Enhancement

The current system has already taken a leap further by identifying the soldier receiving the information by using their heartbeat rhythm as well as sending alert to the crew head in case of emergency. The future of this system if enhanced correctly a proper machine learning algorithm can be developed for analysing various soldier's heart rhythm to avoid false positive results of the soldier's status by enhancing the accuracy of the heart rhythm.

Further, the heart rate authentication can be used as biometric authentication for Soldiers, Captains, Majors, Lieutenants, Colonels, Brigadiers, Generals and other high ranks as well as low-rank officers in the military. This type of authentication helps in improving the standard of authentication provided and increases the security level of the army so that all the +confidential information is safeguarded.

In addition, this type of authentication can also be used in the military's research centres like DRDO (Defence Research and Development Organisation), etc., space research centres like ISRO (Indian Space Research Organisation) and other research centres like BARC (Baba Atomic Research Centre), etc. to protect the research information from enemies.

This leads to the invention of a wide range of IoT based wireless devices and creates a pathway for further invention and discoveries.

References

1. Ramaswamy P, Patnaik LM. Encyclopedia of information ethics and security? 2013.
2. Holder EH, Robinson LO, Laub JH? The fingerprint sourcebook? Dept Justice Office Justice Programs Nat Inst Justice Office Justice Programs Washington DC USA Tech Rep NCJ 2011.
3. Ryoko N, Yu I, Tomohiro U, Masami T, Hiroyasu K, Kazuki J. Biometrics authentication based on chaotic heartbeat waveform? 2014 Biomedical Engineering International Conference 2014.
4. Anil KJ, Ruud B, Sharath P. Biometrics: personal identification in networked society. Springer 1999.
5. Sasikala P, Wahtdabanu RSD. Identification of Individuals using electrocardiogram. Int J Comp Sci Netw Secur 2010; 10.

6. Shen TWD, Tompkins WJ, Hu YH. Implementation of a one-lead ECG human identification system on a normal population. Eng Comp Innov 2011; 2: 12-21.
7. Wang Y, Plataniotis KN, Hatzinakos D. Integrating analytic and appearance attributes for human identification from ECG signals? Proc Iometrics Symp Res Biometric Consortium Conf 2006; 1-6.
8. Biel L, Pettersson O, Philipson L, Wide P. ECG analysis: a new approach in human identification? IEEE Trans Instrum Meas 2001; 50: 808-812.
9. Shen TW, Tompkins WJ, Hu YH. One-lead ECG for identity verification? Proc 24th Annu Conf Fall Meeting Biomed Eng Soc EMBS/BMES Biol 2002; 62-63.
10. Israel SA, Irvine JM, Cheng A, Wiederhold MD, Wiederhold BK. ECG to identify individuals? Pattern Recogn 2005; 38: 133-142.
11. Wübbeler G, Stavridis M, Kreiseler v, Ousseljot RD, Elster C. Verification of humans using the electrocardiogram? Pattern Recognit Lett 2007; 28: 1172-1175.
12. Sufi F, Khalil I, Habib I. Polynomial distance measurement for ECG based biometric authentication? Secure Commun Netw 2010; 3: 303-319.
13. Sufi F, Khalil I. An automated patient authentication system for remote telecardiology? Proc Int Conf Intell Sensors Netw Inf Process 2008; 279-284.
14. Fatemian SZ, Agrafioti F, Hatzinakos D. HeartID: cardiac biometric recognition? Proc 4th IEEE Int Conf Biometrics Theory Appl Sys 2010; 1-5.
15. Singh YN, Singh SK. Evaluation of electrocardiogram for biometric authentication? J Inf Secur 2012; 3: 39-48.
16. Singh YN, Singh SK. Identifying individuals using eigenbeat features of electrocardiogram? J Eng 2013.
17. Chan ADC, Hamdy MM, Badre A, Badee V. Wavelet distance measure for person identification using electrocardiograms? IEEETrans Instrum Meas 2008; 57: 248-253.
18. Juan S, Arteaga F, Hussein AO, Abdulmotaleb ELS. ECG authentication for mobile devices. IEEE Trans Instr Measur 2015; 591-600.
19. Daniel T, Markus Z, Nadine RL, Heike LBME, Christian W, Matthias S. Human authentication implemented for mobile applications based on ECG-data acquired from sensorized garments? Computing in Cardiology Conference (CinC) 2015.
20. Green LS, Lux RL, Haws CW, Williams RR, Hunt SC, Burgess MJ. Effects of age, sex, and body habitus on QRS and ST-T potential maps of 1100 normal subjects. Circulation 1985; 71: 244-253.
21. Vue Z, Junjie W. Practical human authentication method based on piecewise corrected electrocardiogram? 7th IEEE International Conference on Software Engineering and Service Science (ICSESS) 2016.
22. Goldsmith A. Wireless Communication? Cambridge University Press 2005.
23. Yao-Nan L, Li-Cheng C, Yuh SS? A walkie-talkie-like emergency communication system for catastrophic natural disasters? 10th International Symposium on Pervasive Systems, Algorithms, and Networks 2009.
24. Ganesan S. RFID and GPS technology and applications. Workshop Style 2007.
25. en.wikipedia.org/wiki/Global_Position_Syatem
26. Ramani R, Vlarmathy S. Vehicle tracking and locking system based on GSM and GPS? Intel Sys Appl India 2013.
27. Bell J. Basic GPS navigation. Practical Guide to GPS Navigation 2008.
28. Shreenivas J, Sutanoe MS, Bhushan J, Vrushali B, Jinesh N, Astiva A. Implementation of a system for localization and positioning of vehicles using GPS and GPRS technology? Int J Fut Comp Commun 2014; 3.

*Correspondence to

Anuradha M

St. Joseph's College of Engineering

Tamil Nadu

India