A Communication-Architecture for Life-Critical Data Transfer in the BITS-LifeGuard Wearable Computing Environment

Rajiv Ranjan Singh[1], Rahul Banerjee[2]

Abstract: **This paper discusses a communication-architecture for transferring the life-critical data by the wearable computer to the vehicular computer in the BITS-LifeGuard environment. Communicating life-critical information poses a set of complex issues with respect to the initiation, tracking and termination of the processes / functions including the information extraction, access to authorized users, integrity of the data and above all security involved with the information. We have created an experimental setup in which the identified requirements of the communication architecture are being tested and validated. The validation will also take care of the effect of noise and any interference which may be present in a vehicle's environment**

***Index Terms*— BITS-LifeGuard, Noninvasive Sensing, Road Safety, Wearable Computing, Bluetooth.**

I. INTRODUCTION

ROAD safety is a major concern for the researchers and governments worldwide as it has led to the loss of millions of precious lives. Such accidents on the highways as well as on semi-urban and rural roadways can take place due to a variety of reasons like those emanating from mechanical failures in the vehicles, driver's ignorance or negligence of the safe driving practices and non-compliance with traffic rules and regulations, apart from accidents that may take place due to unexpected or unanticipated errors on part of someone other than the driver. However as the various published surveys and related research show, quite a large number of fatal road accidents take place due to slower reflexes of the vehicle's driver which may possibly arise out of mental or physical fatigue caused due to several reasons like consumption of alcohol / intoxicants beyond what is considered safe for driving, long driving hours and prolonged mental stress [1], [2]. The Royal Society for the Prevention of Accidents (RoSPA) [3] has published sizeable data that helps to find the threshold levels beyond which driver fatigue needs to be carefully tackled in order to prevent driver originated causes of fatigue including those arising of slower reflexes or errors of judgment. It is important to note here that such problems can be handled in many ways including the following: (a) by use of wearable computers alone (b) by use of a hybrid approach wherein sensors appropriately embedded into the vehicle's environment as well as mounted on driver's body (embedded in a fabric-based flexible wearable clothe). In order to solve this problem, physiological measurement of select parameters indicating the fitness of drivers for driving helps in continuous monitoring of relevant parameters for avoiding accidents. The critical information extracted is also helpful in generating some kind of alert to the driver is possible. This can also provide necessary information needed by the recovery agencies in case a road accident occurs in spite of all efforts [4]. In addition to sensing devices the system needs signal conditioning circuits, communication devices (for both in-vehicle and to outside agencies), processing units etc. that put together forms a part of a larger pervasive computing environment.

II. RELATED WORK

BITS-LifeGuard and BITS-HeartGuard are the constituents of the 'Project BITS-WearComp'† which is a long term ongoing research and development initiative of the Centre for Software Development (CSD), BITS Pilani in the area of proactive human-centered computing. The BITS-LifeGuard system is being designed as a wearable computing system that could act as a personal safety device for the automobile drivers. Apart from the ability to continually monitor the relevant critical data obtained through a variety of non-invasive sensors, the device shall also have wireless communication capability and an ability to alert the vehicle's driver in time for taking up necessary action for preventing any possible accidents [5].

[1]*Rajiv Ranjan Singh is with the Centre for Software Development at the Birla Institute of Technology & Science, Pilani, Rajasthan, INDIA. He is currently pursuing his Ph.D. in Wearable Computing at BITS Pilani. He can be reached at rrsingh@bits-pilani.ac.in*

[2]*Rahul Banerjee is an associate professor of computer science at the Birla Institute of Technology & Science, Pilani, Rajasthan, INDIA. He also leads the Centre for Software Development at BITS Pilani. He can be reached at rahul@bits-pilani.ac.in*

† Project BITS-WearComp Homepage may be accessed at the URL: http://discovery.bits-pilani.ac.in/wearcomp/

The BITS-LifeGuard like all other constituents of the 'Project BITS-WearComp' does take advantages of the problem space partitioning. Fig. - (1) shows the handling of person-specific requirements by the proposed system involving two necessary computing elements: (a) driver's wearable computer and (b) the vehicular computer. In both the elements different communication units have been provided to take care of intra-vehicular and inter-vehicular communication. Both of these elements have backup memory as well as backup processing facility for providing robustness. The wearable computer has to assess the driver's health status as well as any such information which may otherwise be indicating his inattention or fatigue during driving. In order to do this the wearable computer is expected to collect inputs from its sensors and generate an alert to the driver if needed after processing the relevant information.

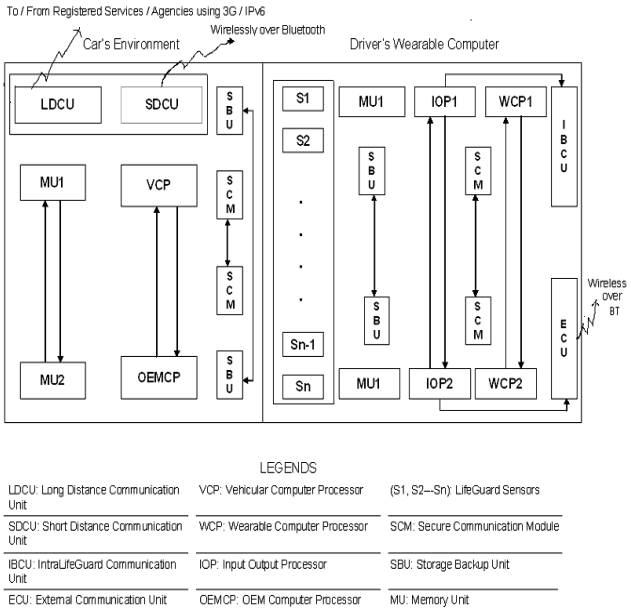

Fig. (1): Functional blocks of the Pervasive Computing Environment of the Vehicle and the Wearable Computer

Once the wearable computer infers that even after being alerted, the driver doesn't take the expected action in time the vehicular computer shall receive an SOS signal from its wearable counterpart. The vehicular computer may have several additional roles to play including the support for GPS and GIS data manipulation, interpretation and taking the vehicular control once the SOS has been received. The system can also help in the rescue of the driver if all efforts towards accident avoidance fail and if the vehicle meets with an accident [6].

As mentioned by Thad E. Starner, the BITS-LifeGuard design not only attempts to take care of the wearability aspects but also tries to address the issues of privacy and security of the vehicle driver. It can act as a personal health repository of the driver and could facilitate the exchange of critical medical parameters to the agencies whosoever may need it [7].

III. PROBLEM DEFINITION AND MOTIVATION

Wearable computing dates back to 1970s when they were designed and built as assistance devices. Such devices may use the combination of mobile multimedia, wireless communication and wearable computing techniques. One of the promising applications of wearable devices has been for health status monitoring of patients, athletes etc. as they will be always worn on the body. By measuring the physiological signals such as heart rate, respiration rate, electrocardiogram, body temperature, and S_pO_2 etc., several applications have been built to monitor the health status of a person. These physiological signals if collected from a vehicle driver's body with the help of a wearable computing unit, could reflect his health status as well as his state of inattention, drowsiness etc. during drive time.

However, in order to communicate various sets of values of critical parameters that are required for carrying out a reliable analysis within the wearable computer and sharing some of these measurements as well as inferences with pervasive computing environment of the BITS-LifeGuard system, it is essential that a mechanism is created for transferring the related data over the wired links within the wearable, over the wireless links between the wearable and its environment and wirelessly with the select elements in its environment in a way that satisfies the following requirements:

- verifiable data integrity
- verifiable data authenticity
- data tracking
- maintenance of confidentiality

The steps required in the process are varied and depend largely on the specific critical importance of the data to be captured, used and transferred. These include making design decisions involving the following:

- Identification of the set of parameters which are to be measured directly or indirectly.
- Choice of the data-subset that requires intra-wearable communication and the subset of the data –subset that requires post-processing may be needed to be transferred to any other element within the pervasive computing system environment referred in the foregoing sections.
- Identification of set of the critical parameters / data related for which system needs availability of one or more of the following features:
  - verification of the transmitting and receiving entities (authenticity check)
  - an assurance of no unauthorized modification in the data originally sent (integrity check)
  - verification of the rights of the elements placed outside the wearable for receiving the data (authorization check)

Therefore, it is clear that select physiological signals must be preferably captured through non-invasive sensing methods and information needs to be extracted as per the design specification before acquisition, processing and secure real-time data transfer can be carried out within or outside wearable computing environment.

IV. OUR ADDITIONAL CONTRIBUTIONS

Although several approaches have been tried by researchers as well as productized by some companies, to this date none of them have been able to provide a foolproof system design to this effect. Traditionally, two approaches have been taken: (a) modifying the vehicle's environment by embedding additional sensory devices in the vehicle itself; (b) placing the sensors on the body as an embedded set of constituents of the wearable computer. We have chosen the wearable computing approach because stress, fatigue, drowsiness, slowing down of reflexes etc. have been found as the major causes of road accidents and wearable computers will be obviously helpful in estimating the related parameters by analyzing a set of physiological signals using body mounted sensors. Wearable computing if combined with certain other characteristics like (a) driver's behavioral profile, (b) environmental conditions (during drive time) and (c) proactive warning systems would provide an acceptable solution for the identified problem.

V. SECURE REAL-TIME COMMUNICATION ARCHITECTURE

BITS-LifeGuard Communication architecture is required to fit within the generic framework provided by the 'Project BITS- WearComp' architecture [6]. Although each of the elements depicted in the proposed overall pervasive computing environment (Fig.-1) may have an independent role, the information sharing between these elements shall be possible by proposed design discussed in following sections.

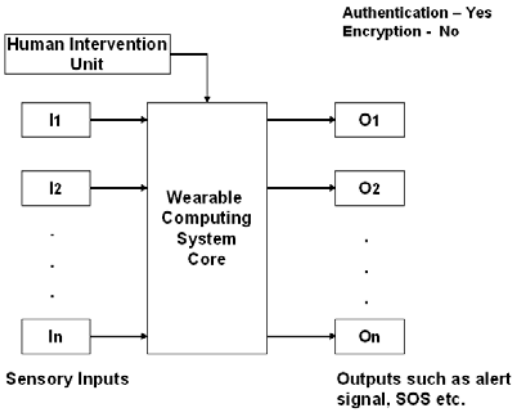

Fig. 2(a): Communication between elements of Wearable Computer itself

The wearable sensors placed on the driver's body will be communicating to the wearable computing system core (mostly wired but it is likely that some wireless sensors may also be used). The physiological signals acquired from these sensors would be processed by the wearable computing system core and necessary outputs such as alerts to the driver, an SOS to the vehicular computer via the external communication unit could be generated as shown in Fig.-2(a). Since the communication is within the wearable itself, no encryption of data is needed after authentication process succeeds.

The vehicular computing system core may take its inputs from External Communication Units (ECUs) of the wearable computer or the vehicle's pervasive computing environment which may be passing through at any point of time and thereby forming a Personal Area Network (PAN) of such wearable computing system cores as shown in Fig.-2(b). In this case, for having a secure communication, both authentication and encryption are needed for avoiding unwanted access by unauthorized entities in the vicinity of the host vehicle.

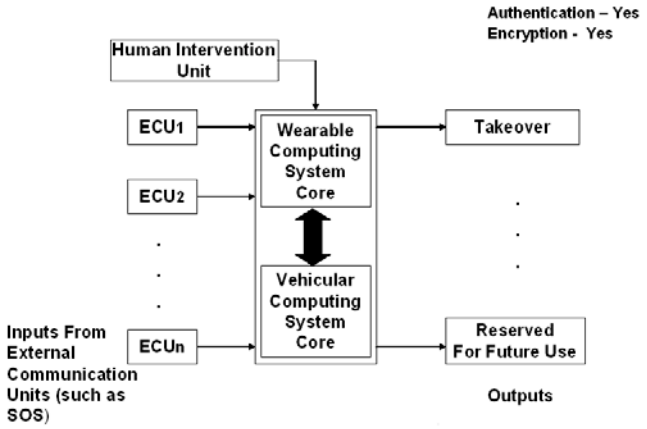

Fig. 2(b): Communication between elements of Wearable Computer and Vehicular Computer

In order to share important relevant data to the outside agencies including the recovery agencies, a third set of communication link is needed which will take its inputs from the Short Distance Communication Units (SDCU), which is communicating with ECUs of the wearable computer while the Long Distance Communication Unit (LDCU) communicates with the outside world.

The information thus collected must be processed and an appropriate action must be initiated (such as alert to external agencies, searching for medical help etc.) as shown in Fig.-2(c). This requires a foolproof authentication and encryption mechanism, since the information is not only shared by the personal area network but also by the external agencies. Any misuse of information may mislead the recovery agencies and will not serve the very purpose of the design.

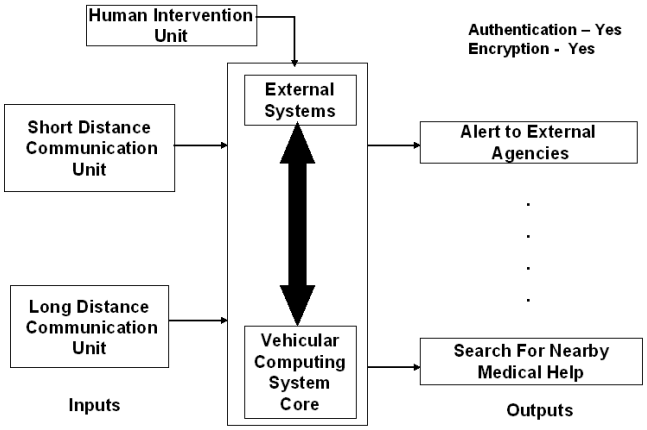

Fig. 2(c): Communication between elements of Vehicular Computer and Outside World

In all the three communication blocks the Human Intervention Unit (HIU) is expected to take care of the requirements wherever the situation so demands. As it can be seen from these diagrams that the interaction between the wearable computer and the vehicular computer will be achieved via PAN technology such as Bluetooth whereas the communication between the vehicular computer and the outside world will involve any of the 3G technologies. Each device will have its own IPv6 address for ease of identification, routing and tracking of communication from / to them in the Mobile Network scenario.

VI. IMPLEMENTATION

In order to test the early implementation of the first phase of the above referred communication architecture, we are using a simulated environment by using Intel XScale® based handhelds as the wearable computer and the Intel® Pentium® M Processor with enhanced Intel® SpeedStep technology as the vehicular computer. However, we are aware that the actual vehicular computer shall require a special purpose microprocessor / microcontroller using a real-time operating system. We are therefore separately studying these aspects and shall try to create such a physical test environment in the second phase of our experimentation. Both of the physical devices used in our current experimental setup have in-built Bluetooth radio units which can be used for the short-distance communication with each other. At present we are using the Bluetooth API provided by Microsoft for Bluetooth device discovery etc. We also use windows socket programming for communication over Bluetooth in the current setup. However in our final setup we may use a different set of choices depending upon field trials and the performance parameters required to be adhered to.

VII. EXPERIMENTATION AND PERFORMANCE EVALUATION

As discussed in the foregoing sections the experimental setup had to handle security as well as performance aspects expected of any such real-time communication system which required a reasonable degree of security due to the targeted system's life-critical nature.

The experiment is designed on the following lines:

- Get the time stamp of message generation and start of message transmission at the sending machine.
- Get the time stamp of start of reception of message, receipt of the complete message and time required to process the message (where possible) at the receiving machine.
- Generate a short acknowledge (ACK) message and measure the similar parameter at both sending and receiving nodes.
- Collect the information at both the nodes about number of transmission errors noticed (if any), profiling of time and memory if possible.
- Introduce external noises / source of errors, simulate real life environment and test all the above referred parameters in the presence of external disturbances / noises /interference. These noises may include:
    (a) Noises generated by noise generators / signal generators as may be available in the local electronics lab.
    (b) Noises generated through microwave ovens, IEEE 802.11 LANs, HomeRFs etc.
    (c) Noises generated due to spark plug activities automobiles and other common environmental disturbances (as may have been recorded in literature)

The steps required to design the communication protocol are as follows:

- Creation of explicit message and binding each such message with one of these codes like control codes, request codes, response codes and error codes etc.
- Defining consequent states and labeling them.
- Defining transitions from one stage to the other until goal state is reached.
- Reachability analysis to be performed and protocol verification to be done.
- Finally timing and sequence diagram will be generated and validated.

As analysis of the figures 2(a), 2(b) and 2(c) itself reveals that three different sets of security solutions are required to be implemented for intrawearable communications, wearable-vehicular computer communications and vehicular-external world communications. A careful analysis of all the three requirements has indicated that while all the three do require respective authentication mechanism, cryptographic solution is not needed in the intrawearable communication / data transfer, private key cryptography is adequate for wearable-vehicular computer communication / data transfer and public-key cryptography

is required to be combined with private-key cryptography for vehicular computer-external world communications. A separate experiment have been planned to be carried out in near future for addressing these aspects of secure real-time life-critical transfers.

VIII. CONCLUSION

As evident from the foregoing discussion, evolution of an acceptable model for secure real-time data transfer for life-critical applications involving wearable computers has several challenges involved. While several successful and partially successful wearable computing systems exist, most of them have not so far focused on this critical requirement. Therefore the presented work which is still in progress shall be able to make an important contribution to the existing body of knowledge in this area.

REFERENCES

[1] European Transport Safety Council, "The Role of Driver Fatigue in Commercial Road Transport Crashes," Technical Report, ISBN: 90-76024-09-X, European Transport Safety Council, Rue du Cornet 34, B-1040 Brussels, 2001.

[2] NCSDR / NHTSA Expert Panel on Driver Fatigue and Sleepiness, "Drowsy Driving and Automobile Crashes," 1998. [Online]. Available: http://www.nhlbi.nih.gov/health/prof/sleep/drsy_drv.pdf.

[3] The Royal Society for the Prevention of Accidents (RoSPA), "Driver Fatigue and Road Accidents: A Literature Review and Position Paper," February 2001. [Online]. Available: http://www.rospa.com/roadsafety/info/fatigue.pdf

[4] Rahul Banerjee, "The BITS LifeGuard System," First Technical Meeting European Commission's Next Generation Network Initiative project, Brussels, June 2001.

[5] Rahul Banerjee, "An Innovative Architecture for Wearable Computer System for Saving Human Lives from Road Accidents," HiPC International Conference, Workshop Session on Cutting Edge Technologies, Bangalore, December 22, 2004.

[6] Rahul Banerjee, "From Research to Classroom: A Course in Pervasive Computing," IEEE Pervasive Computing, Vol. 4, No. 3, pp. 83-86, July-Sept. 2005.

[7] Thad E. Starner, "Wearable Computing for the Developing World," IEEE Pervasive Computing, Vol. 4, No. 3, pp. 87-91, July-Sept. 2005.