Wearable Computing Challenges

Ajay Parbhu
University of Auckland
apar164@aucklanduni.ac.nz

ABSTRACT
Computer technology has been an important aspect in our lifestyle for many years. There has been continual development in making the devices we use smaller and more portable, whether it is laptops or mobile phones. However these devices aren't necessarily suitable for some situations, sometimes we need something smaller or more accessible, wearable computing strives to fill that niche. Wearable computing offers us with a means to constantly gather data and provide real time feedback. It is a device that will always be present with the user and accepts the input of commands while the user is engaged in other activities. This article discusses the numerous challenges that revolve around wearable computing. The lack of power efficiency, types of communication networks, interface design and security implementation, are the main issues that will be discussed. We will also discuss the solutions that have been proposed by other researchers, such as turning sensors off when they're not needed; switching networks based on task, means of integrating interfaces in a non-obtrusive manner, and light weight encryption technologies.

INTRODUCTION
The introduction of wearable devices has shown great results for gathering and reporting information in a non-intrusive manner. Users no longer have to give their full attention to a computer device, one of the goals of wearable computing is to remove this attachment and allow for computations to be completed without any user involvement.

The key to developing such device lies in the developer's ability to solve or work around certain problems. This report will give an overview of the challenges that must be overcome for developing a successful wearable computing device. Power consumption of the system is an important aspect; we want the device to have enough power for computation but not too much as to require batteries that weigh the user down. Communication should be reliable and suitable for a given task. Storing and sending information should be done in a secure manor to uphold privacy. The interface being presented to the user should be non-obtrusive and should be simple to use no matter what activity the user is completing.

POWER
The majority of issues that arise when developing a wearable computing device spawn from the main problem of power management [10]. This has been a problem for many years and is where a lot of the research is going for wearable computing. We can link the issues presented in this paper, and other minor issues with power management:

- Communication – reliability and speed, cost power when it comes to networking
- Security – requires computation for encrypting information
- Interface – having a user friendly interface can often cost a lot of power to operate
- Weight – more power can require more batteries, therefore more weight

[8] Evaluates the power issues that occurred when implementing a health monitoring system for patients. Their device contained batteries that would be the source of power, when calculating the amount of battery life the device should be operational for; they found they were off by a big factor (24-48 hours required, 10 hours actual). [8] Decided to re-evaluate their device and removed some of the unnecessary functionality, the LCD output for displaying the results of the data that was collected was removed. They also considered a different method of calculating the battery life but have yet to implement it (see future work).

The batteries that are used are an important factor in the power efficiency of the device. [8] explains the use of having an "ideal battery" in which the voltage is constant through discharge and has constant capacity for each load value, this is important as the device should only accept a constant power output as to not waste any energy or be underpowered. They believe that devices that implement non ideal batteries have poor performance and an inconsistent estimate on how long the battery will last.

There has been development on how to better manage the power in a wearable device. [10] Believes that most conventional systems fail to manage their power supply very efficiently, and that the CLAD (Cross-linkage for assembled devices) system is a solution to this problem. Most wearable devices contain many sensors which record data, however they are unable to regulate which sensors should be turned on or off. They believe that there are situations where having all the sensors activated is wasting power (such as having the GPS on in your own home). Their design is supposed to fix this problem by controlling

the power intake of the sensors, and turning sensors off when they are unneeded.

Power failure is also an issue; sometimes components of a device or the whole device itself can lose power and therefore shut off. This can be disastrous if the data being collected is of high importance [8]. [10] Devised a solution for when certain sensors have failed, it revolves around the idea of having pseudo data being generated which can fill in the gaps where there has been a failure. This gives the device enough time to correct the power issue, or send a message to the user alerting them of the problem without recording any outlying data.

INTERFACE

The interaction between the user and the device is something that must be taken into consideration. We must ensure that the interface that is presented to the user is simple and easy to use without imposing any restrictions to the users every day activities, therefore the integration should be seamless [12]. Many of the problems that revolve around creating an efficient interface for a device spawn from the same problems involved in creating the device in the first place. Size of the interface is directly related to the size of the device itself, having a small interface can lead to users having trouble operating the device and deterring them from their activity [2]. The power consumption of the device also influences the interface. Having a fully responsive interface with screens and buttons can sap immense power from the devices batteries, most designers attempt to find the right balance between an easy to use interface and power consumption [3].

Some problems are however, unique to the interface of the device. The location of the interface on the system is also something that must be considered. Having the device placed on the user in an awkward area can cause problems; people want to be able to easily operate the device at any point in time with minimal effort [1].

The output of information is also important for interface design and not just the input. Having the results from the gathered data being displayed to the user through an interface is an important issue as users prefer to have the data being relayed to them in a non-intrusive manner [14]. [11] Decided to go with a vest in which the user can wear, the device is placed inside of the vest and can easily be accessed (see Figure 1). The user is easily able to quickly detach the device and view the information in a smooth and elegant gesture, this interface has very little intrusion with the user completing every day activities, in this case maintaining aircrafts.

Figure 1: Aircraft maintenance workers vest

[13] Have developed a set of glasses which are able to display information to the user directly in front of their eyes, this is a very effective interface for the user as many people already wear glasses and therefore there is seamless integration between the user and the device. The ability to have the information where ever you look is also a pleasing factor as it gets rid of the need of having a display that must be taken out of hiding to view.

COMMUNICATION

Communication between wearable computing devices and a control system is an important aspect in the usefulness of wearable computing. As with interface design, communication networks for devices also follow the same problem set as many other challenges. Power is the main issue here, the amount of energy required to send data from one location to another is quite taxing [7]. Therefore developers have designed there devices to be more efficient in their means of transferring data. [7] Uses the amount of signal processing and the deadline for the data to be sent to formulate the amount of energy required to send the information. Having a deadline means data will not be transferred instantly, this way, rather than sending three or four small packets constantly, we can send one big packet. If the deadline is quite long, and requires very little signal processing, the amount of energy to send the data can be quite low, therefore saving power.

There are two main methods for transferring data that has been collected from a device to another system for processing. One method of doing this is to simply retrieve the device from the user once they are finished with it, and then proceed to evaluate the data; this may not suit all situations however. In doing this, we have discontinuous processing; sometimes we require continuous processing in which the data is required to be sent all the time from the device to the system. Continuous transmission of data requires a constant network connection, [4] describes the

use of having a Bluetooth connection to relay data to and from the device. Bluetooth was chosen due to it being fairly economical to implement and it requires very little power to operate. It is also partially secure, the frequencies in which the connection lies on are generated randomly, and this helps to prevent attackers from listening in on the device. Encryption is also used; secret keys are passed around to authorized users that are able to turn data that is normally illegible, legible. As many devices already have Bluetooth readily available, it allows for quick integration with many other devices. There is little need for engineers to develop technologies that can receive and communicate with the device as the technology is already there.

Bluetooth is only one of the methods that these devices can use to transmit information; there are many other methods such as GPRS (general packet radio service), WLAN (wireless local area network) and UMTS (universal mobile telecommunications system) [9]. [9] Tries to utilize all of these methods and select the best method for the devices task or location. Their main goal was to establish a programming model in order for developers to easily select which type of network would be required. This solves problems around power, security, reliability of connections and speed of the connection, by allowing for developers to create applications that can pick the best connection for a given task. If there is a high priority task that is required to be run, it can be run on the connection that has the most reliability and speed at the cost of power. If the task is of low importance and holds data that isn't very important, it can be run on whatever connection is available without the overhead of finding the most ideal connection and not having to encrypt any information.

SECURITY

As wearable devices are able to continuously collect and store data, one key issue is the ability to securely keep or transmit this information. Security is vital for devices that contain sensitive information, the data is either stored directly on the device, or is sent to another system for storage and processing. The storage and the communication between the device and system must therefore be secure.

The connection between the wearable device and an outside service can be secured in many ways, one of which is to implement an authorization system in order for the user to prove their status before connection [6]. This method is, however computationally intensive, as proving your identity costs power to send and receive messages. [6] Have developed a method to remedy this issue, their idea comes from using different authorizations based on the context the user is in. If the user has a connection through a secure wireless network, the amount of security computations will decrease. If the user is connecting via something more insecure, such as a public hotspot, the amount of security computations will therefore increase.

The storage of data within the device is also a potential security hazard; [8] developed a device that stores medical information. If the user of the device was to misplace it, others could potentially pick the device up and access the information. Encryption plays a key role here, if we encrypt our data when we record it, others will have a harder time accessing it. This encryption however requires computational power and therefore we're limited in the strength of security we apply.

[5] Have developed a lightweight identity-base encryption protocol which allows for the device to securely send and store information on the device. They found that generating encryption/decryption keys is a great solution to securing data transactions. If the data that is being transferred is the same for multiple nodes (updating nodes with current status), there is a distinct peer-wise key for each of the transactions. This use of encryption is quite taxing and therefore they resulted in using a common key for the repeated transfers, this means instead of generating a new key set for each similar transaction, they used just one. This therefore led to less processing and more efficient power management as well as security.

METHODOLOGIES AND FINDINGS

[7] began testing their energy model by having body sensors equipped to the waist and upper body, the sensors are there to detect whether the user is falling or not. If one of the sensors detects that the user is falling, it sends the signal to the other node, in which that sensor will reply with its evaluation on the user falling or not. The nodes then signal their data to the base system. The connection to the base system, the power, signal processing and deadline of the connection are the factors that were tested during the experiment. Different networks were used to test their model; they used Zigbee, Bluetooth, Wi-Fi and UWB (Ultra Wide Broadband) as the connections for the node.

The results show that the deadline plays a very important factor when it comes to power management. They first established a 20ms deadline (time in which data needed to be sent), not enough data was collected in this delay. By turning the deadline up to 3 seconds, they were able to get a 4 times improvement in power saving compared to just one second. This is important as it allows for developers to judge whether or not they want to trade power for a faster relay of data. They also found that UWB offered the best speed to power ratio when implementing their idea, it allowed for a double in the order of magnitude in energy savings as opposed to Bluetooth.

[9] Managed to develop a concept with a modular design allowing for future wireless technologies to be implemented very simply by developers. They managed to integrate it within an IDE, which has proven to be quite useful with other developers that were new to this design. They also found their use of code generation for allowing different connection protocols to be implemented benefited beginner

developers. The generated code was also helpful for creating more complicated constraints for experienced developers.

[11] Decided to test their new technologies by using interviews, surveys and questionnaires. They found through the interviews that the use of a portable device which can hold technical documents was very useful. Cabin log books were something that maintenance workers frequently would refer to; they used to be printed in books. They then switched to a terminal in modern aircrafts that were fixed to a certain area. Having a device that could house these books and be portable was something that was found useful during the interviews. Users having their hands full while trying to complete tasks was also something that was brought up during the interviews. Users didn't like trying to pull out their heavy and obtrusive PDA's from their pockets, they preferred the method of having a vest which could house the device.

[10] had two goals; one was to manage the power of different sensors, and to generate pseudo data for data consistency. The first goal was tested by implementing their device onto an accelerometer unit and then testing the power consumption of the system while increasing the number of sensors. They found that without the CLAD device, the power consumption did not change at all while the number of sensors increased (see Figure 2). This was due to the fact that the sensors would always be active. They then attempted the same experiment, but this time with the CLAD device on the system. The power consumption of the system started off quite low (.15 with one sensor with the device compared to .55 with one sensor without the device) and then gradually increased. This therefore showed that there was a decrease in power consumption with their device. There was however an increase in power when the amount of sensors used went above 5, this was due to the overhead introduced by CLAD.

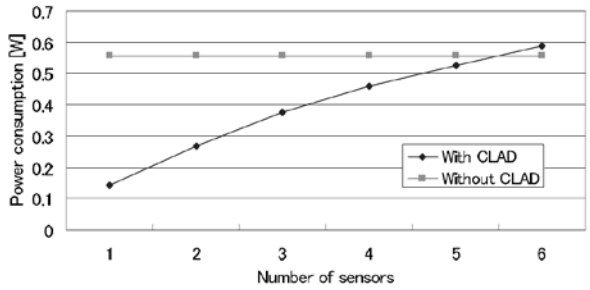

Figure 2: Power Consumption vs. No. Sensors graph for CLAD

The second goal was tested by having multiple sensors attached to a person's hips, wrists and ankles to record their acceleration. They had 5 sensors overall and tested the accuracy of the data being recorded when one or more of the sensors was deactivated. They tried every combination of deactivating the sensors (31 in total) and recorded the results. They found that the accuracy stayed around 70-80% for all but two of the sensors being operational for their AA (All Alive) implementation of the pseudo data generator.

FUTURE WORK

[8] Found that the estimation techniques that were being used to determine the power consumption of their device may not have been very accurate. They are attempting to use a dynamic power consumption rating to test the efficiency of the device. They also plan on implementing an EEG (Electroencephalography) device to go along with their current ECG (Electrocardiography) device.

Power efficiency is still a major factor that still requires a lot of research. If we can find various solutions to this issue, many of the other issues are automatically solved. Future work into creating smaller and lighter power sources is also something that should be considered. This would allow for more devices to be developed that are less intrusive to the user.

[11] Plans on evaluating their device with user feedback on their prototypes. They have already completed interviews and now plan on conducting workshops for various users to gather more information on how to improve their device. They also wish to implement their technologies on other computing systems, with computers getting smaller and faster, they believe that their technology would improve on newer devices.

[7] Found that their initial implementation of network selection had a few minor bugs. One of which introduced an unknown delay when switching connections. They believe that this is due to insufficient data being stored before sending and they intend on finding the cause of this issue. Obviously, once the issue is identified, solutions will be implemented to circumvent this problem as well as keeping the power efficiency of their application.

CONCLUSION

The continual development and use of wearable computing devices has introduced various challenges. These challenges must be overcome in order for users to be able to integrate wearable computing into their everyday lives in a seamless and non-intrusive manner.

The above readings point out various issues with the current devices today, as well as possible solutions to fixing those problems. Power efficiency seems to be the major issue among the devices, along with communication, security and interface design. Notable solutions to the power problem involved switching certain sensors on the device off when not needed. Communication and security solutions revolve around ideas that would better enhance the power efficiency of the device due to power being a limiting factor. Ideas ranged from switching the networks that a device could be connected to in an effective manner and using a lightweight encryption method instead of other more intensive approaches.

REFERENCES

1. Anliker, U., Beutel, J., Dyer, M., Enzler, R., Lukowicz, P., Thiele, L., and Troster, G., A systematic approach to the design of distributed wearable systems. *Computers, IEEE Transactions on*, (2004), 1017-1033 DOI: 10.1109/tc.2004.36.
2. Bainbridge, R. and Paradiso, J.A., Wireless Hand Gesture Capture through Wearable Passive Tag Sensing. *Body Sensor Networks (BSN), 2011 International Conference on*, (2011), 200-204 DOI: 10.1109/bsn.2011.42.
3. Blasko, G. and Feiner, S., A menu interface for wearable computing. *Wearable Computers, 2002. (ISWC 2002). Proceedings. Sixth International Symposium on*, (2002), 164-165 DOI: 10.1109/iswc.2002.1167243.
4. Bouhenguel, R., Mahgoub, I., and Ilyas, M., Bluetooth Security in Wearable Computing Applications. *High Capacity Optical Networks and Enabling Technologies, 2008. HONET 2008. International Symposium on*, (2008), 182-186 DOI: 10.1109/honet.2008.4810232.
5. Hamdi, M., Boudriga, N., Abie, H., and Denko, M., Secure wearable and implantable body sensor networks in hazardous environments. *Data Communication Networking (DCNET), Proceedings of the 2010 International Conference on*, (2010), 1-8 DOI: DOI: 10.1109/tc.2004.36.
6. Lindstroem, J., Security challenges for wearable computing - a case study. *Applied Wearable Computing (IFAWC), 2007 4th International Forum on*, (2007), 1-8 DOI: DOI: 10.1109/tc.2004.36.
7. Loseu, V., Ghasemzadeh, H., and Jafari, R., A wireless communication selection approach to minimize energy-per-bit for wearable computing applications. *Distributed Computing in Sensor Systems and Workshops (DCOSS), 2011 International Conference on*, (2011), 1-8 DOI: 10.1109/dcoss.2011.5982156.
8. Martin, T., Jovanov, E., and Raskovic, D., Issues in wearable computing for medical monitoring applications: a case study of a wearable ECG monitoring device. *Wearable Computers, The Fourth International Symposium on*, (2000), 43-49 DOI: 10.1109/iswc.2000.888463.
9. Megen, F.v., Timm-Giel, A., Salmre, I., and Goerg, C., Smart Networking Requests: Supporting Application Development Relying on Network Connectivity for Wearable Computers. *Applied Wearable Computing (IFAWC), 2006 3rd International Forum on*, (2006), 1-12 DOI: DOI: 10.1109/dcoss.2011.5982156.
10. Murao, K., Takegawa, Y., Terada, T., and Nishio, S., CLAD: a Sensor Management Device forWearable Computing. *Distributed Computing Systems Workshops, 2007. ICDCSW '07. 27th International Conference on*, (2007), 46-46 DOI: 10.1109/icdcsw.2007.28.
11. Nicolai, T., Sindt, T., Witt, H., Reimerdes, J., and Kenn, H., Wearable Computing for Aircraft Maintenance: Simplifying the User Interface. *Applied Wearable Computing (IFAWC), 2006 3rd International Forum on*, (2006), 1-12 DOI: DOI: 10.1109/dcoss.2011.5982156.
12. Raghunath, M.T. and Narayanaswami, C., User Interfaces for Applications on a Wrist Watch. *Personal Ubiquitous Comput.*, (2002), 17-30 DOI: 10.1007/s007790200002.
13. Spitzer, M.B., Rensing, N.M., McClelland, R., and Aquilino, P., Eyeglass-based systems for wearable computing. *Wearable Computers, 1997. Digest of Papers., First International Symposium on*, (1997), 48-51 DOI: 10.1109/iswc.1997.629918.
14. Stein, R., Ferrero, S., Hetfield, M., Quinn, A., and Krichever, M., Development of a commercially successful wearable data collection system. *Wearable Computers, 1998. Digest of Papers. Second International Symposium on*, (1998), 18-24 DOI: 10.1109/iswc.1998.729525.