Grade: 70%

1 Introduction

Commented [CCT3831]: Title of Paper?

Quality healthcare is regarded as an important service for the physical and mental health and well-being of people. With technological advances in the medical area and advances in the energy efficiency of continuous sensing, more convenient, cost effective and efficient options are being explored. One particular technology, Wireless Body Area Networks (WBANs) have stated to emerge in the medical field. A WBAN is a network of wireless nodes worn on the body that are capable of sensing and computing. Examples of WBANs in everyday life include smartwatches and fitness bands (Ragesh and Baskaran 2012b).

As with most new technologies, problems arise along with the benefits they supply. In the case of WBANs, monitoring patients is being made easier and more efficient. However, by using a wireless network, the security of medical information and the patient is at risk (Dimitriou and Ioannis 2008; Afshare 2015). Therefore, despite the vast benefit WBANs provide, they are outweighed by the problems they raise and therefore should not be used in healthcare. This report will review the technology, cover the arguments expressed by both sides and provide a solution to address those concerns.

Commented [CCT3832]: Outline your arguments and briefly mention what your solution is in the thesis statement.

2 Technology

A Wireless Body Area Network is a collection of sensors, also known as nodes, that are linked together to provide information about environment (Fourati 2014). In medical care, these WBANs are used to monitor a patient's condition and keep the doctor up to date with the patient's condition. The sensors can monitor a patient's temperature, heart rate, blood glucose levels, and many other signals (Karulf 2008; Yu 2009; Silicon Labs 2013). These signals are then sent to a central server where doctors can monitor them to ensure the patients is in good health.

The information the sensors obtain is wirelessly transmitted to a central control unit located on the human body. This unit is responsible for getting the information from all of the sensors and sending it wirelessly to a central server, which is what the doctors will have access to. A common example of a central control unit is a smartphone. To ensure safety, the central control unit gives each node a unique key when the node enters the network. Only nodes with these unique keys can access, change, or provide data. When a node leaves or enters the network, the central control unit gives each node a new key. This guarantees once a node leaves a netwrok, it can no longer change or read data (Malik and Singh, 2013; Chin *et al*. 2012).

Commented [CCT3833]: How does this paragraph strengthen your argument? Background context should only be included if it is necessary to make your point.

3 Argument for Using Wireless Body Area Networks

Wireless Body Area Networks is a technology that has been developed to ease the jobs of medical staff and recovery of patients. This section will take a look at this technologies benefits.

Commented [CCT3834]: Usually unnecessary to include this as an intro to each section

3.1 Reduced Labor Costs

In healthcare, WBANs can be used to save time and human resources. Because patient information is all being sent to a remote server, doctors are able to monitor all the patients from a single location, Furthermore, by using machine learning techniques, this process can be automated and extremely accurate. By automating the monitoring process, the number of medical staff required to be checking on patients is reduced.

Commented [CCT3835]: Reference?

3.2 More Healthcare Availability

Research has been done to explore a method of having patients monitored by doctors while living at home (Ragesh and Baskaran 2012a). By facilitating home healthcare, space in hospitals can be increased allowing for more individuals to receive treatment. The effect of heaving more available healthcare is tremendous. For example, 30% of deaths worldwide are caused by cardiovascular disease, most of which could have been prevented with proper healthcare (Latré *et al*. 2011). With WBANs becoming ubiquitous, healthcare can be provided to many more people and the number of deaths for cardiovascular disease can be reduced.

Commented [CCT3836]: Be more specific. What kind of research?

Commented [CCT3837]: Logical gap here. How do WBANs facilitate home healthcare? Do you have a reference?

3.3 Cost Effective

Today's common medical equipment comprises of large machines that are specialized for the task they do. Due to thier specialized design, replacing these machines often restricts the medical facilitaties options, making replacing these machines expensive and inefficient. On the other hand, WBANs are made up of small and inexpensive sensors. The functionality of these sensors is very general and can be applied t measure a variety of signals. Therefore, replacing these sensors is easy and cheap (Darawich and Hassanien 2011).

Commented [CCT3838]: But can WBANs replace these large machines?

3.4 Supporting Arguments Conclusion

WBANs have proved to be an alternative to traditional healthcare monitoring methods. They provide an easier and cheaper method of monitoring patients while at the same time offering healthcare to more people. In spite of WBANs being so beneficial in providing healthcare, they having a crucial downfall. WBANs are susceptible to attacks. When relying on technology to administer healthcare, it is vital for the system to be secure for the safety of the patient.

4 Argument Against Using Wireless Body Area Networks

WBANs use wireless technology which sends data through the air.This means the data is able to be intercepted by an attacker and used for their benefits. This section analyses some of the problems associated with the use of this technology in greater detail.

Commented [CCT3839]: Vague

4.1 Types of Attacks

WBANs use wireless technology to send and receive data. Wireless technology is susceptible to attacks because the attacker can get access to the network from a remote location close to the network. The attacks can be categorized as either outside or insider attacks. Outsider attacks occur when the attacker cannot join the network because all the nodes have unique keys.

Instead, the attacker acts as a bystander and launches attacks such as passive eavesdropping, denial of service attacks and replay attacks. On the other hand, insider attacks occur when the attacker is able to get physical access to a device that is part of the network. Getting access to the device will give the attacker an approved key, giving the attacker much more power. The attacker can get access to medical information, and has the ability to tamper with data packets.

Commented [CCT38310]: Only list the attacks that will be discussed further

4.1.1 Outsider Attacks

Passive eavesdropping requires the attacker to listen and record messages from a node. These messages are encrypted, however with enough messages, the encryption can be cracked and the messages revealed. Replay attacks occur when messages from two nodes are recorded and resent from the attacker. This results in a node receiving multiple identical messages, which would cause the node to repeat certain procedures. These procedures could be administrating certain medication to patients, which could potentially lead to an overdose. Denial of service attacks can be made by sending lots of data to overload a server. By overloading a server, it would stop the server from receiving messages from sensors and result in patients going untreated (Al Ameen, Liu, and Kwak 2012; Dimitriou and Ioannis 2008; Gupta, Mukherjee, and Venkatasubramanian 2013).

4.1.2 Insider Attacks

Insider attacks are a much more dangerous type of attacks. Being able to access a node in the network allows the attacker to have access to all the medical information that passes through. This information can give the attacker details of a patient's health which they can use to harm the patient with other attacks. Attackers also have the ability to change the output messages from the sensors. These messages could be different from the actual patient information and can result in the patient's problem going unnoticed. Attackers also have complete control of the node and therefore are able to withhold data packets that pass through their node. Lastly, they can change the patient's profile information, resulting in medical staff potentially misdiagnosing the patient (Al Ameen *et al*. 2012; Dimitriou and Ioannis 2008; Gupta *et al*. 2013).

4.2 Opposing Arguments Conclusion

An attack to a Wireless Body Area Network can result in a patient going untreated, being misdiagnosed and having their healthcare information stolen. These potential dangers that arise from using WBANs are dangerous enough to not use WBANs in medical facilities. An alternative solution should be sought after.

5 Recommendation

A solution to the use of WBANs is to avoid wireless networking and use wired networks in medical locations where sensitive material is kept. By using a wire connection, attacking the network and obtaining information becomes a much more difficult task (Dunham 2011). Rather

than being able to infiltrate the system from a location close to the medical facility, the attacker would physically have to get access to a computer inside the building to do any damage. However, hospitals are kept protected by security and being able to get access to server rooms is a difficult task. Despite the good WBANs provide, they are unsafe to use for medical diagnoses, treatment and monitoring. Previous methods should be used where all the sensors and hardware containing data had no wireless capabilities.

Commented [CCT38311]: Solution could use more detail. Try to find a more balanced and nuanced response that does not simply suggest removing WBANs from healthcare.

A potential critique of this recommendation is that while many technologies have security flaws, they are still in use. An example of this is online banking, where sensitive information is being sent wirelessly. To this, the counter can be made that banks keep logs of all transactions so if money is stolen, it can be reversed and the damage undone. WBANs on the other hand cannot undo damage. If an attacker uses an attack to make it appear that a dying patient is healthy, the damage done is not reversible. For this reason, the risk of attacks is one that should not be taken.

6 Conclusion

WBANs are an emerging technology that utilize sensors to monitor their environment. WBANs have been applied to a medical setting to monitor patients. Sensors in the network monitor signals in their surroundings and send that data to a remote server, creating a convenient and cost effective procedure compared to current convention. However, WBANs are susceptible to attacks which would compromise confidential information. This creates the argument as to whether the convenience of easy monitoring of patients and reduced labour cost is worth the risk of security information. As a recommendation, WBANs should not be used in medical facilities, but rather machines with no wireless capabilities. Thus, eliminating most the risk of data theft and manipulation.

Commented [CCT38312]: Nice summarization of paper