

WIRELESS TECHNOLOGY: IT'S ROLE IN MILITARY COMMUNICATION TO EMPOWER DEFENSE OF A COUNTRY

Aaryan Dambe

Ram Ratna International School

Abstract

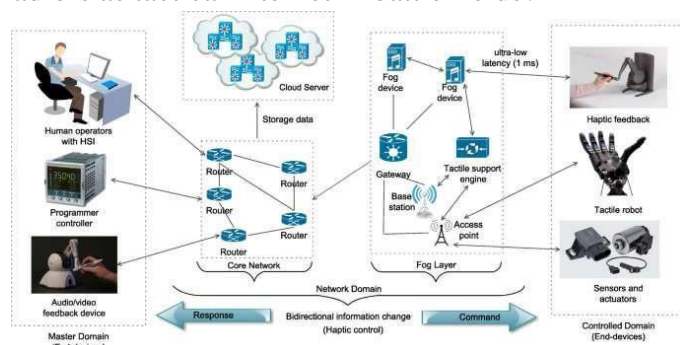
Ever since the birth of wireless technology by Guglielmo Marconi in 1896, it has been used for the military purposes, communication, and the safety of soldiers. The technology has been favoring humanity every time they needed it, but as time flies, the modernization around the world made the fast-paced growing wireless technology look lingering. Therefore, this paper focuses on how can wireless technology be used to improve military communication, and how it can be optimized for the soldiers survival and safety monitoring, making use of wireless technology for different compartments of military defenses of a country; for example in alarming system of intruders in the army bases.

Keywords: *Headquarters deployment augmentation, leap, cluster base, Joint Tactical Radio System (JTRS), Tactile internet.*

INTRODUCTION

This paper is mainly intended to implement the role of wireless technology to empower the military communication and country's defense. Wireless technology, such as in cell phones, uses radio waves to transmit and receive data; It is used increasingly for data transmission. The military tried several ways to upgrade their wireless technologies, but listed below are some improved methods for it to be implemented for the country's defense like wireless sensor network, integrated sensors deployment in soldiers vest ,using joint tactical radio systems for better communication , usage of DoD's of country defense , etc. Communication plays a vital role in military defense system and there are still many ways to improvise upon it through different emerging technologies, but these have magnetized negative attention from the malignant enemies of country who are supposed to infiltrate the sensitive data of government servers and the transmitted signals from the wireless sensor system for their own gain, which can be referred as military cyber-attacks. Consequently, in this paper we are going to discuss:

- 1) How can we make Usage of New/Old radio`s as tactical internet in battle fields?
- 2) Different ways for advancing the soldier communication and safety vest
- 3) How we can use the wireless sensor network as alarming system?
- 4) Wireless sensor system threats which occur
- 5) Valid solution as unmanned vehicle to reduce the threat faced by wireless sensor system.

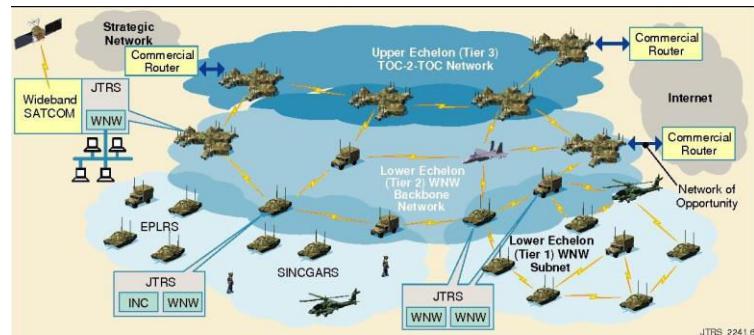


Theory

1) How can we make Usage of New/Old radio's as tactical internet in battle fields? When it comes to strengthening a country's defense, the first thing which comes to our minds is military security, thus becoming much more significant while war or combat training to rookie soldiers. About the usage of the radio, we can use the joint Tactical Radio System (JTRS). JTRS is a family of radios and a family of communications waveforms designed to be interoperable and provide military forces with next-generation systems for digital voice and data communications during military operations. It will let our soldiers focus on making commanding decisions, rather than giving voice transmission of their location. Now this technology will transmit radio text messages back and forth between individual combat elements in real-time, which are regularly translated on to a digital map background on to the user's compact computers. This type of communication will build a tactical internet; combining a different types of SINCGARS (Single Channel Ground and Airborne Radio System) and making usage of Joint Tactical Radio System which will create a better improvised army technical architecture, and the leading commanders having the 'troop codes' will make the software of JTRS easy to alarm the other troops of commanders.

Basically tactile internet is a sub-class of an IOT (internet of things) which helps an basic/advance technology to work by abnormal way for example through hand gestures, eye contact, through brain impulses, etc. So firstly, the plan could to control the

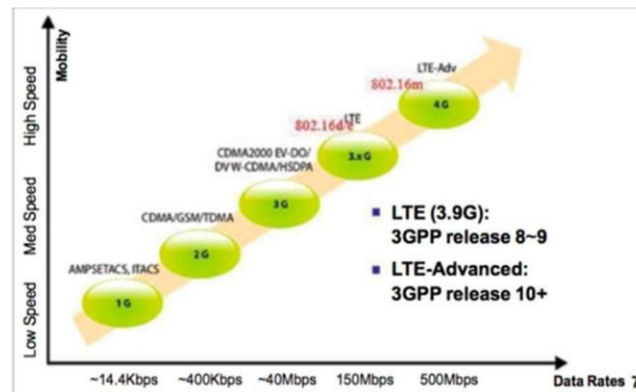
radio software through brain impulse, because if on the battlefield the commander is injured and is struggling to move his hand so he can easily alarm the army base/headquarters through brain with the help of tactile internet. These kind of technologies can be also be used like:-





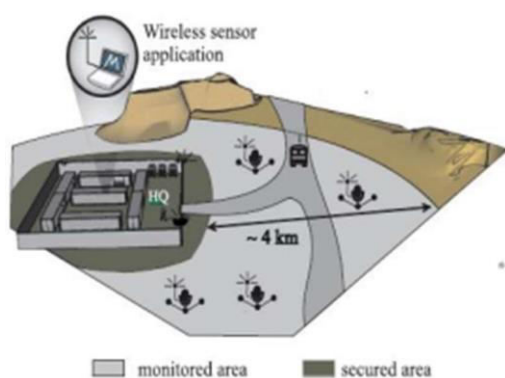
However, it can be also added that the Joint Radio System, can be used in Headquarters deployment augmentation with the signals from the compact device of soldiers; therefore, the headquarters can easily deploy their troops at the emergency point where the other commander needs help or backup.

Now, the main problem occurs after brainstorming on the solution, the accumulation of the higher frequencies, larger bandwidth and greater sensitivity to anchor the uninterrupted network. The answer for this question may be the LTE (Long Term Evolution) which is being used in our mobile phones and communication devices. The LTE can be combined with the military communication devices, which will end up being beneficial for the military as it makes the network much safer, and gives multiple deployment bandwidth of 1.4 MHz, 3 MHz, 5 MHz, 10 MHz, 15 MHz, and 20 MHz. The LTE has got several notable advantages that states - The flexibility of LTE allows it to be used in both land and maritime defense applications. Video streaming for increased situational awareness is a crucial component of network-centric warfare. Defense users may be able to take use of advanced current hardware and software solutions that have demonstrated commercial performance in a variety of physical situations, ranging from broad open countryside to congested metropolitan areas.



2) Different ways for advancing the soldier communication and safety vest. Military utilization has an enormous numbers of data flow through sensors. They need a data median that can join the necessitates, of a single data stream that can integrate video feeds from drones targeting radars with intercepts from mobile phones. More sensors may now be integrated into soldiers' systems with less weight, size, and battery consumption. As the defense industry is turning up all the tables to a new generation of technology quicker, inexpensive, and more flexible communication. The communication is now adhered wirelessly directly to the war fighter for the country's defense. Therefore, the military needs a highly modernized vest which will give them all essential system in a easy access. A vest which has many technologies like the retractable night vision, blast detection monitor, navigation sensor, health monitor, GPS, JTRS radio, etc. The vest will give the soldiers local and remote spectrum monitoring and surveillance system, and Global Positioning System (GPS) protection against spoofing and jamming

threats. The vest will be consisting of a central compact computer which will be controlled by the soldier to access the system for information, for example:- if the soldier wants information about their location so the computer will execute its command to drag down the particular system to come under the soldiers control by displaying its location through GPS or the navigation sensor. This control over the central monitor on their arm/wrist would be made uncomplicated by the custom made military software being used by the computer; which will include the most user- friendly options of icon and buttons . The computer screen being touch screen will be making this application much easier to use and if the soldiers needed will be even trained for the usage of the software application. Computer may look some like this:-



Wireless Sensor network based military monitoring |

Experimental

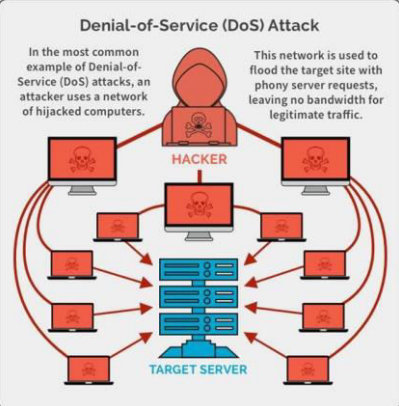
3) How we can use the wireless sensor network as alarming system?

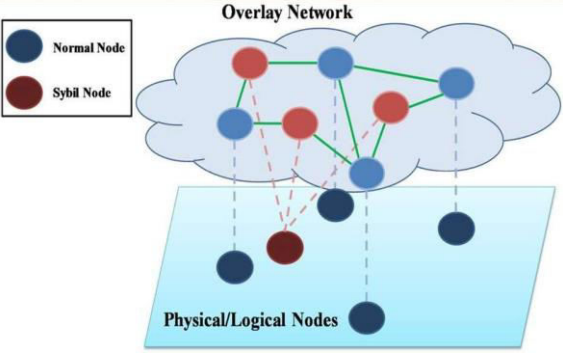
The main function of the wireless sensor network is to observe the enemy movement and synchronize the activities of the army .The nodes (it's a sensor node which is capable of performing some processing

, gathering sensory information, and communicate with other connected nodes in the wireless sensor nodes) will be deployed at the place we want to monitor in the given range as the figure shows. There will be also an

base station in the headquarter(HQ) to control the nodes and collect, process, and analyze the information from the various nodes. The nodes are connected with various sensors to sense the environment for enemy movement and coordinate with the soldiers for the same. There are various kinds of sensors which are connected to the nodes, like camera sensors which detect the motion, face and scene of the enemy in the quickest and the clearest way possible for the nodes. It also uses MEMS (Micro-electro-mechanical systems) sensors for friend-or-foe identification for the enemy, who conquers and this information is passed to the soldier during the emergency by the base station .The nodes connected with the sensors will periodically send message to the base station in the case of any suspicious activity. Then the base station will receive the information from various nodes and will take the necessary actions like notifying the commando for that particular area or give messages to nodes surrounding that area .

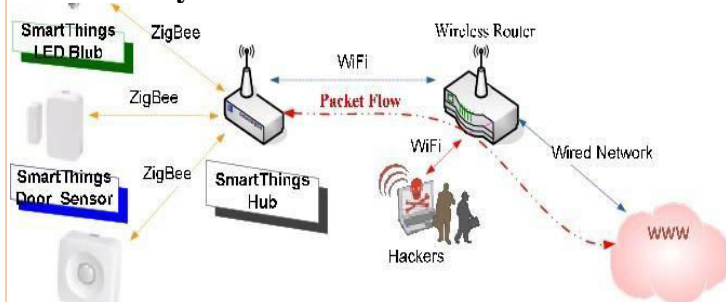
4) Wireless sensor system threats which occur due to its security issue?
 There are several security issues found in the wireless sensor system; here are its few issues which can cause threat to the military :- (In the table below) |

Types of the security issue	Brief explanation about the threat
<p>Denial of Service Attacks</p>  <p>Denial-of-Service (DoS) Attack</p> <p>In the most common example of Denial-of-Service (DoS) attacks, an attacker uses a network of hijacked computers. This network is used to flood the target site with phony server requests, leaving no bandwidth for legitimate traffic.</p>	<p>In our case, it a malicious act where a malicious user who tries jamming our nodes.</p> <p>In easy terms it uses spamming to our nodes continuously to confuse them. Or in other case it can spam several inappropriate messages to the particular node to create collision with the radio signals which consist an appropriate messages.</p>
<p>Sybil Attack</p>	<p>In our instance, the malicious user create a small number of entities</p>

 <p>Overlay Network</p> <p>Normal Node Sybil Node</p> <p>Physical/Logical Nodes</p>	<p>who are the clones of the multiple original nodes. This will consists of some share of the system, and this will let the hacker get many node Id's which gets produced to get closer to the network they want to overlay and intercept its message routing which creates a lot of traffic in the</p>
--	---

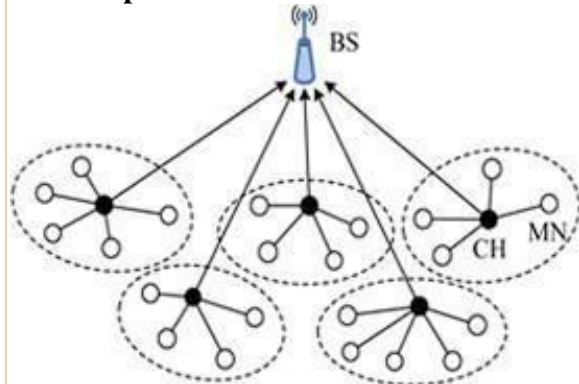
military network.

Traffic Analysis Attacks



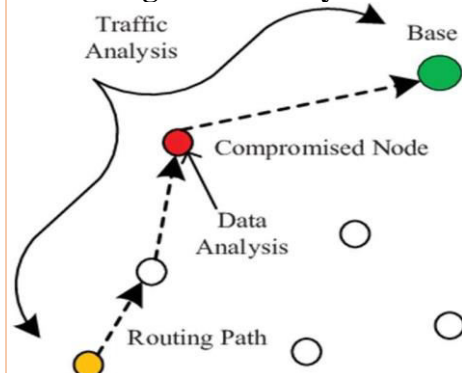
It is method of the enemy which follows the flow data packets from nodes to nodes to understand its pattern, and to know its main node which is nearest to the base station and sends all the information.

Node Replication Attacks



It may feel the same way as the Sybil attack but in this instance the node is added the original wireless sensor system and clone the other nodes already existing and this can only change functionality of the network between the nodes and the base station.

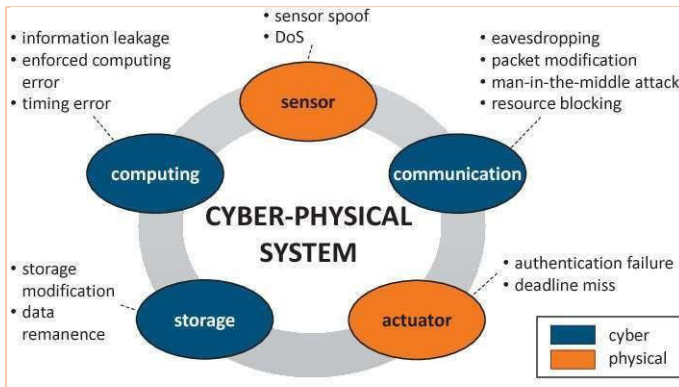
Attacks Against Privacy



In our case, this attack can be taken place after the traffic analysis attack the malicious user may track the node and take out their needed information like the coordinates of the critical areas.

Physical Attacks

It is a method or act the enemy's use to physically enter the environment to alter the hardware of the



device. In our case, it will be the enemy's coming to alter the sensors of the nodes by destroying it or by reprogramming it in their own way.

5) Valid solution as unmanned vehicle to reduce the threat faced by wireless sensor system.

A solution to all this security issues which can cause threat to the military will be the notion of the unmanned vehicle controlled by a wireless sensor network in the military. This vehicle can traverse through the network and observe the network security. The vehicle will be made compact so it doesn't get any attention of the enemy. It will be controlled by the mote inside itself, and with a movable characteristic it can check the reported specific area to know if it is an emergency or a security attack issue. The node has infinite power therefore it can be undertaken for maintenance. There can be several features added to it like a camera for letting the base station soldiers get a brief look at the situation occurred or the night vision to keep the security of the stable notes, different type of sensors. The importance of localization is to link the vehicle location to the base station location. We can use GPS, with the global positioning information we

can finalize our next movement. The driver mote will send the sensor information to the other motes and wait until they reply the position from the base station through the motes. Aside from the navigation, the driver mote has additional responsibility such as deploying motes and maintaining the wireless sensor network.

Let's take a case where the wireless sensor network is divided into clusters. Every cluster will contain a set of motes in the specific area. The set of motes in the cluster will decide it's leader who will be named as the cluster head. The head will entirely bundle up all the messages from the cluster member. To keep the security's issues in mind, we will be following the LEAP key management. The LEAP has four sets of keys from which two we have is from the individual key and the cluster key. The individual key will distributed to all the nodes before deploying it which will help them to encrypt messages they want to send to the base station or the unmanned vehicle mote. The base station and the unmanned vehicle has the other two keys to decrypt the encrypted message send by the stable nodes. The sensor reading of the environment made by the motes will be encrypted by the cluster key and send to the cluster head ; then the base station will decrypt the information with the help of cluster key and then it informs the further steps needed to be taken.

Consider the instance that infrared sensors are equipped by the all the motes to identify the movement of the intruders in our area. These nodes will send the message to the cluster head and then the cluster head will report this to the base station . Suppose the base station wants to cross check whether or not the event did really happen. It will move the unmanned vehicle mote to the region it is rumored to have emergency with the help of GPS or surrounding sensory location. The motes in that area will be equipped with the sensors, which will collect all the important data and sensory information from the encircling and pass it to the vehicle mote. After collecting all the data the vehicle will immediately send the same precise values to the base station. The base station will then compare the values and if it is made out to be different, they can take acceptable actions like informing the soldiers in charge of the nearest troops or activate the mines etcetera. Further the vehicle mote can be used to understand the situation better by using its advance tools like camera or alternative sensing device .the vehicle mote and the base station have direct communication with all proper encryption methods since they both are powerful and have infinite battery life. We charge the battery life of the vehicle with the use kinetic energy due to its movement of wheels.

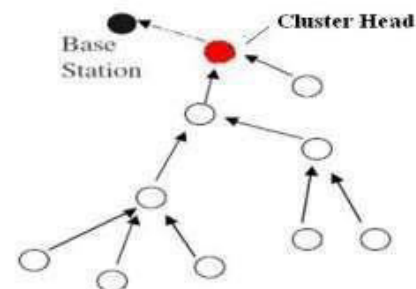
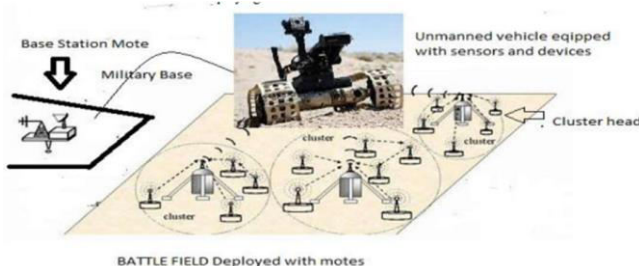
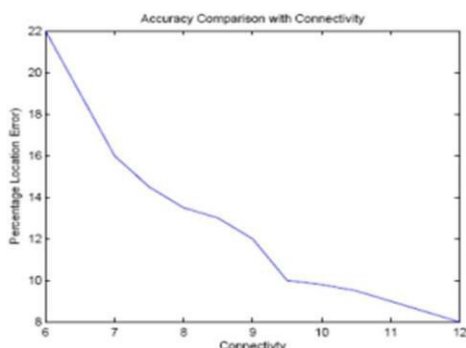
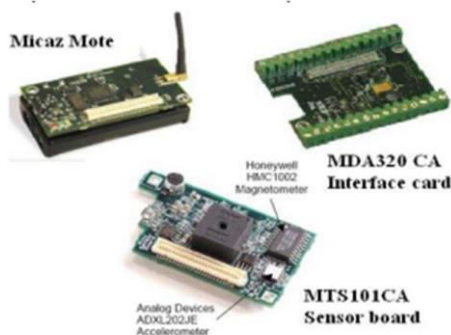


Figure 3. Data aggregation by Cluster head



6. Wireless Sensor network based military monitoring.



The Mote, Interface card and Sensorboard [User Manual].

Now coming to the implementation of this unorthodox unmanned vehicle mote, firstly listing up its hardware needed would be the mote, the interface card and sensor board. These components specifically can be used :- Speaking of software now, as the software used in the base station and on the wrist of soldiers' vest could be a custom made operating system with its IT sectors or TinyOS which is a real time operating system designed for these kinds of applications, which need many additional programming in it like to navigate the vehicle to a particular location, to program it to analyze the sensor data, etc. The result of wireless Sensor network usage in the military system was quite impressive, here is a line graph for the reference :- (on the right side).

Conclusion

Communication is a key part of every country's military system and making this communication wireless makes the soldiers free of dangling wires and even increase their mobility while in emergency. Now the wireless technology has emerged so brightly that the military can now easily reply wireless sensor network for the analysis of a particular area or the border. But due to the greater usage of it, there are cyber-attacks done on the motes and the unmanned vehicle. This is done to gain sensitive information of a particular country or the government done by the enemies to go through it during the need of war time. It can be even done to distract the country from a bigger threat set up by the rival country. But as the time passed, we did create several solutions to improvise on the wireless sensor system and will continue doing the same until we find the world's most secure military system. At the end I would like to say that the military should optimize the wireless technology at its upmost but should always keep the physical backup of wired and human-based application for communication and analysis because the best prepares for the worst situation.

Acknowledgement

I would like to express my gratitude to thank to MISA to conduct this competition where I came to research about many incipient things about Wireless technology and how to make a research paper. Withal I would appreciate the fact that MISA MUN specially made a group designated "MISA Luminous Spark'22" in which they kept updating all the important things we would want to know. Secondly, I would give a great thanks to



my school, Ram Ratna International School and the Principal Mrs. Jaya Parekh and vice principal Mr. Manish Hegde to let us know about this competition and even scholastic mentors as Mrs. Deepa and Mrs. Sanchita, who were availing me for any material required to take part in this competition and determinately I additionally got an abundance of appreciation from my family to take part in this research paper which is very generous of gratitude to me.

REFERENCES

- [1] <https://www.encyclopedia.com/computing/news-wires-white-papers-and-books/wireless-technology>
- [2] <https://blog.isa.org/leveraging-dod-wireless-security-standards-automation-control>
- [3] <https://www.militaryaerospace.com/communications/article/16710748/wireless-devices-link-soldiers-on-the-digital-battlefield>
- [4] <https://www.electronicsforu.com/market-verticals/aerospace-defence/wireless-technology-defence>
- [5] (PDF) Constraints and approaches for distributed sensor network security (final) | Nasrin Yahyaei - Academia.edu
- [6] https://www.cisco.com/c/dam/en_us/solutions/industries/docs/gov/Wireless_Connectivity_De_fense-2.pdf
- [7] <https://www.sciencedirect.com/topics/computer-science/sybil-attack#:~:text=A%20Sybil%20attack%20is%20defined,and%20function%20as%20distinct%20nodes.>
- [8] <https://journals.sagepub.com/doi/full/10.1155/2014/402541>
- [9] <https://arxiv.org/pdf/2007.07646.pdf>
- [10] <https://cradpdf.drdc-rddc.gc.ca/PDFS/unc28/p520923.pdf>