IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)
e-ISSN: 2278-2834,p- ISSN: 2278-8735.Volume 15, Issue 6, Ser. I (Nov - Dec 2020), PP 36-43
www.iosrjournals.org

Jampack: An Enhancement in Design of Tactical Manet And Manpack Transceiver

Sanyatjeet Pawde
Department of Electronics and
Communication Engineering
SRM IST Kattankulathur
Chennai, INDIA

Aditya Garg
Department of Electronics and
Communication Engineering
SRM IST Kattankulathur
Chennai, INDIA

Abstract *– MANETS have been used by the armed forces tactical communication in the battlefield. They provide dynamic connectivity without the requirement of any pre-existing infrastructure. There are times when our news media which is responsible for delivering news of every moment to the general public, jeopardizes the secrecy of certain tactical information, notions of strategic importance and even the lives of our Armed Forces personnel via live broadcast, just for the sake of TRP ratings. To prevent instantaneous broadcast of this clandestine information by the media houses we propose to enhance the existing MANET used in tactical environments by equipping every infantryman on the field of operation with a portable manpack transceiver integrated with ECM(electronic jamming) and ECCM(FHSS) equipment. In the presented work, a schematic representation of Manpack transceiver with integrated jammer circuit is designed and explained. Finally, different scenarios for ideal and jammer operation in a GSM based service on demand network is simulated and analyzed in Riverbed Modeler Academic edition 17.5.*

Keywords *– MANET, ECM, ECCM, Manpack Transceiver, Jamming, FHSS.*

Date of Submission: 20-12-2020 Date of Acceptance: 03-01-2021

I. INTRODUCTION

In our country military operations during a terror attack or a war are heavily covered by the Indian media. In such cases we have often seen that some news agencies, just for the sake of raking huge TRP's deliver highly secretive military information to the general public. Sensitive information such as positions of the armed personnel, when broadcasted on the national television is viewed by the enemy and gives them the advantage over our forces in the operation. This negligent reporting by the media jeopardizes the secrecy of the tactical information and notions of strategic importance and hence the whole operation altogether.

Previously, in some cases even the precious lives of our armed force personnel were compromised because of such actions. Such clandestine information can also be used by some notorious elements of our country for their own benefit to cause havoc and disruption in the country.

A few examples of such incidents:-

During the *2008 Mumbai terror attacks*, Ten Pakistani terrorists trained from the Lashkar-e-Taiba stormed buildings in Mumbai, unleashing a 60-hour siege with automatic weapons and grenades. While the siege was taking place and our National Security Guards (NSG) were trying to end it, an NDTV reporter, in order to get better coverage, went onto the roof of the building next to where the our sniper were positioned and the reporter broadcasted their location on live television. This information was viewed by the perpetrators in Pakistan who communicated it to the terrorists in the building. If this information hadn't been leaked the siege could've ended much faster by our forces.

Another such incident of reckless reporting was during the *Kargil war in 1999*, Barkha Dutt, the media person she is, wanted to send some real war footages to her channel in order to push up their TRP. She carried an *irdium* satellite phone into the battlefield which was tracked by the Pakistanis and caused damage to the army posts. She was also constantly asking our soldiers whether she can take one shot of the battlefield & she was declined each time, as the flash from her camera will easily give away their exact position to the enemy. After 3–4 attempts she decided on her own that it's enough & let's give our audience a glimpse of what's happening at Kargil. Due to this, artillery fire was directed by the Pakistani Observer at Headquarter of a formation because the tactical sign post was illuminated by the camera light. One Officer and three soldiers were killed because of her irresponsible reporting.

After the *Uri attack of 2016*, the intel operations footages were shown by some of the media channels in their broadcast. In the video, one of the intelligence officers was recognized by the local Kashmiri public which was then conveyed to the notorious elements.

II. Current Scenario

MANET's provide independent communication services between forward operating base (FOB) and armed forces personnel deployed in battlefield as it is a decentralized network. In the current scenario, each infantryman carries a highly portable device that is connected to the MANET and the Unit Commander [3] is equipped with a device (also a part of the MANET) with greater resources such as CPU, memory and battery, and has access to the command post. So, if the unit commander's equipment malfunctions or is somehow destroyed, the link with the command post is completely disrupted and the communication stops. The need for ECM and ECCM on the battlefield is major factor in Electronic warfare, but bulky equipment (big high power antennas) decreases the working efficiency on the field. Also, single high power equipment is much vulnerable to threats on a front.

III. Proposed Model

We propose to divide the effect of a single high power jammer into multiple small power units/modules and integrate them with personnel's manpack, thus increasing mobility on the ground and also ensuring effective communication between nodes. Also implement the counter-counter measure technique of frequency hopping within the pack.

Our main objectives are as follows:

1. To enhance the existing MANET used in tactical environments by equipping each individual on the field with independent comms and counter equipment.
2. To design a portable command and control information system,[1][2]
3. To reduce the jammer size using the principle of cell splitting by decreasing antenna height considering the transmission power and mean effective radius of jammer.
4. To integrate communication unit with the counter measure and counter-counter measure unit.
5. To simulate the above mentioned parameters and get the results by considering the parameters as packets sent and received.

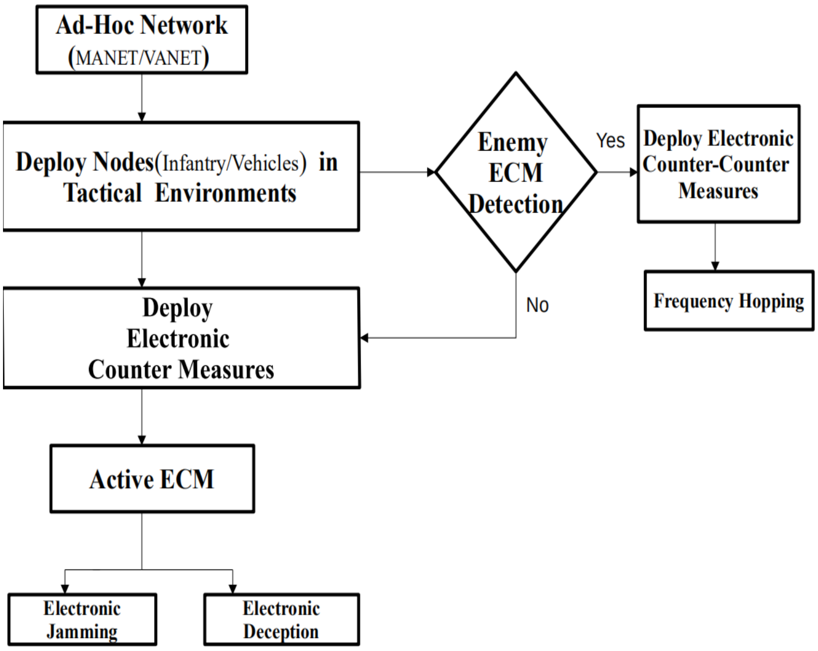

Ad-Hoc Network (MANET/VANET)
Deploy Nodes(Infantry/Vehicles) in Tactical Environments
Enemy ECM Detection
Yes
Deploy Electronic Counter-Counter Measures
Frequency Hopping
No
Deploy Electronic Counter Measures
Active ECM
Electronic Jamming
Electronic Deception

Figure 1: Flowchart of the proposed model.

First, an Ad-Hoc network (MANET) is setup. Each infantryman who would be an individual node of the MANET will have an integrated comms and counter equipment in their manpack. With the help of this network the infantrymen can communicate among themselves and the command post as well.

In order to jam the enemy signals active electronic counter measures such as electronic jamming and deception are used to block any communication surrounding the strategic area so as to safeguard the modus operandi of the mission be it against media DSNG vans(downlink jamming) or brute blocking of entire bands against IEDs. Continuous scanning of operation field is done to detect the enemy countermeasures (DDoS/Channel Interference). If any ECM from enemy is detected the electronic counter-counter measures such as frequency hopping are used to switch to another allotted communication channels.

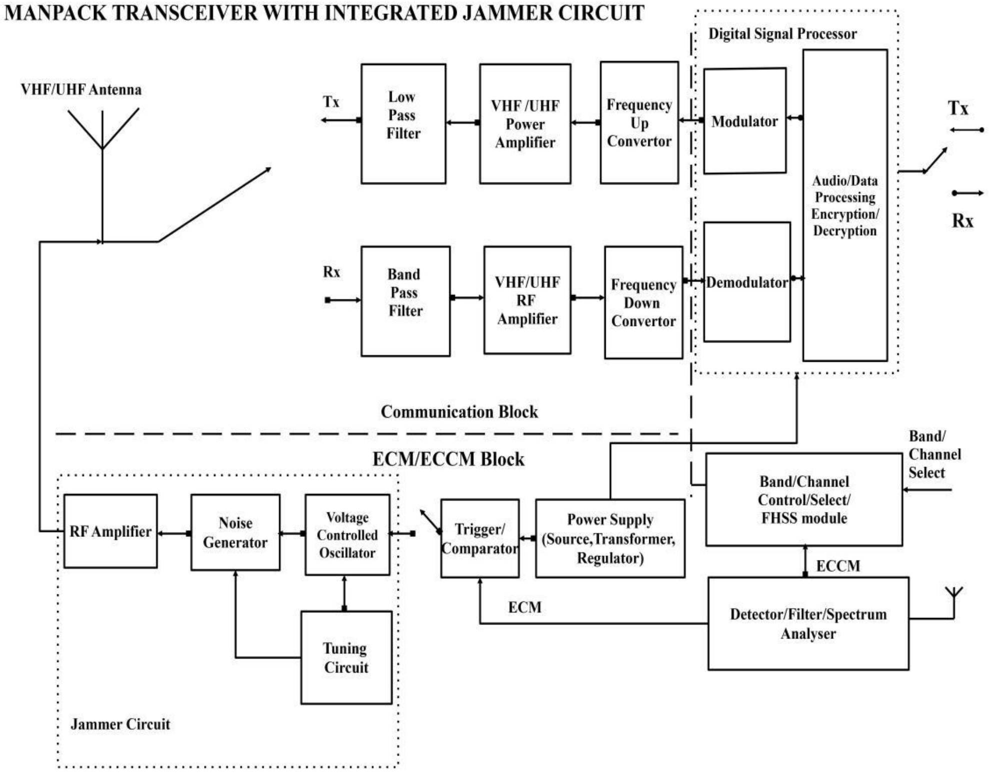


Figure 2: Schematic representation of multiband MANPACK Transceiver with integrated jammer circuit

This is our prototype schematic design depicting the internal circuitry of our proposed model, the working of which is as follows:

Communication Block:

The Communication block will function as it has been in the currently existing models. The optimum frequency for ground tactical communication is VHF/UHF, that is, from 30MHz-3000MHz.

1. The voice or data to be transmitted or received is converted by a ADC/DAC in a Digital Signal Processor which also modulates and demodulates the data.
2. The output from or input to the DSP is of low frequency (Intermediate Frequency) which is up and down converted while transmission and reception respectively.
3. While transmitting this signal is amplified by a power amplifier and passed through a low pass filter to filter the ripple.
4. Similarly, while receiving the signal is passed through a band pass filter so as to allow a particular band of frequency to pass through and then its amplified by a RF amplifier to boost the filtered signal.
5. The signal frequency is then down converted and information is retrieved after demodulation.
6. The transmission and reception modes are controlled by switch mechanisms.

ECM/ECCM Block:

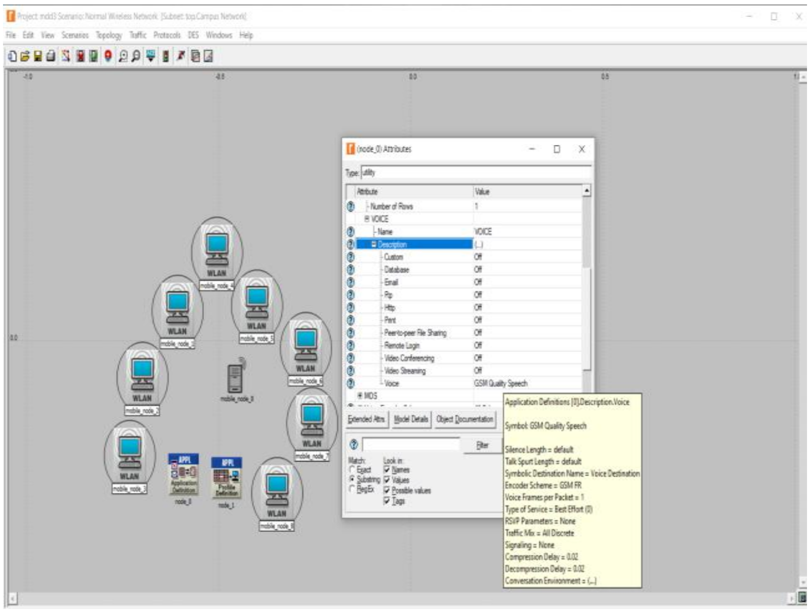
This part of circuitry gives the personnel control of electronic counter and counter-counter measure block of the proposed model.[11]

1. The detector circuit comprises filters tuned to specific frequencies, if a particular frequency is detected by the circuit (with the help of antenna), the triggering circuit gets triggered.
2. The trigger circuit works as a comparator to compare input voltage from the detector and its own fixed input. If the detector voltage is high, the switch closes thus connecting the power supply to jamming circuit.
3. This enables the jamming subsystem; this mechanism is useful as until the frequency to be jammed is detected, the jammer draws no power.

4. Once the jammer circuit is active, the tuning circuitry of voltage controlled oscillator generates that particular frequency which is further boosted by RF amplifier and this boosted signal is radiated by antenna. This is the working of the ECM (counter measure/jamming part).
5. For ECCM (counter-counter measure), any miscreant frequency signal is detected via spectrum analyzer which alarms the operator and turn to band control to hop to a different frequency, the same could be used to switch between VHF/UHF in communication block.

IV. EXPERIMENTATION AND RESULTS

To illustrate the proposed model of dividing the effect of single high power jammer into multiple low power jammers we have conducted a simulation case study in Riverbed Academic Modeler 17.5 Software. We have considered three different scenarios.[10][5]



Type: utility

Attribute	Value
Number of Rows	1
VOICE	
Name	VOICE
Description	(...)
Custom	Off
Database	Off
Email	Off
Ftp	Off
Http	Off
Print	Off
Peer-to-peer File Sharing	Off
Remote Login	Off
Video Conferencing	Off
Video Streaming	Off
Voice	GSM Quality Speech
MOS	

Match: ○ Exact ● Substring ○ RegEx
Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags

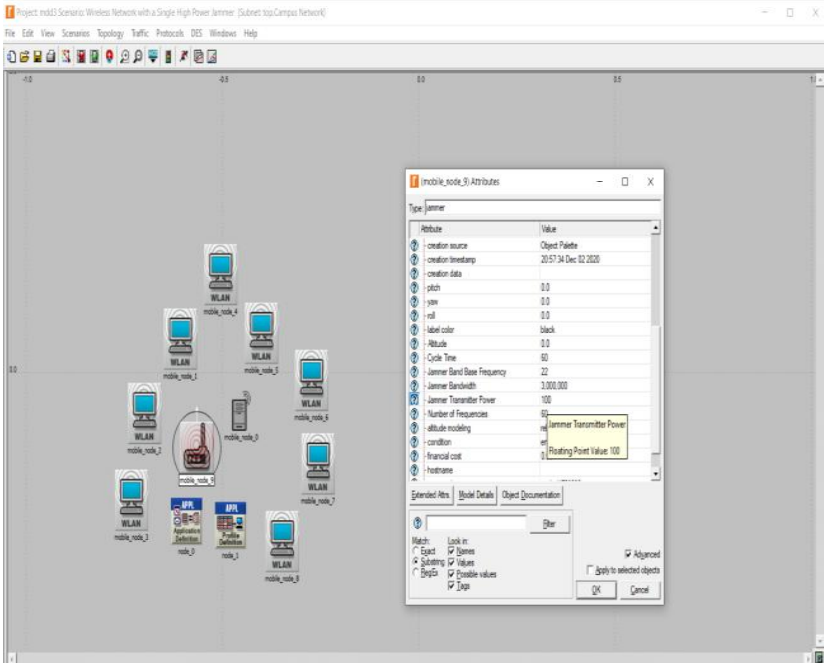
Application Definitions [0].Description.Voice

Symbol: GSM Quality Speech

Silence Length = default
Talk Spurt Length = default
Symbolic Destination Name = Voice Destination
Encoder Scheme = GSM FR
Voice Frames per Packet = 1
Type of Service = Best Effort (0)
RSVP Parameters = None
Traffic Mix = All Discrete
Signaling = None
Compression Delay = 0.02
Decompression Delay = 0.02
Conversation Environment = (...)

Figure 3: (Scenario 1) Normal Wireless Communication Network

Scenario 1: A normal wireless communication network with mobile nodes and a server is designed with the server depicting a mobile tower providing GSM voice service to users.



Type: jammer

Attribute	Value
creation source	Object Palette
creation timestamp	20:57:34 Dec 02 2020
creation data	
pitch	0.0
yaw	0.0
roll	0.0
label color	black
Altitude	0.0
Cycle Time	60
Jammer Band Base Frequency	22
Jammer Bandwidth	3,000,000
Jammer Transmitter Power	100
Number of Frequencies	60
altitude modeling	re
condition	en
financial cost	0.
hostname	

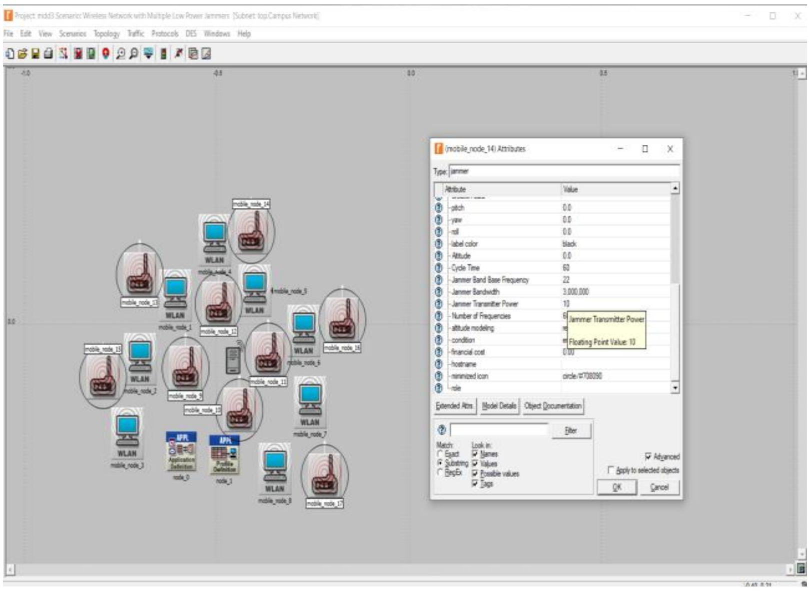
Jammer Transmitter Power

Floating Point Value: 100

Match: ○ Exact ● Substring ○ RegEx
Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags
☑ Advanced
□ Apply to selected objects

Figure 4: (Scenario 2) Network with a single high power jammer

Scenario 2: A single high power jammer is introduced in the network which would interfere with the availability of service analogous to a battlefront where enemy communication is jammed.


Project: mdd3 Scenario: Wireless Network with Multiple Low Power Jammers [Subnet: top.Campus Network]

(mobile_node_14) Attributes

Type: jammer

Attribute	Value
pitch	0.0
yaw	0.0
roll	0.0
label color	black
Altitude	0.0
Cycle Time	60
Jammer Band Base Frequency	22
Jammer Bandwidth	3,000,000
Jammer Transmitter Power	10
Number of Frequencies	6
altitude modeling	
condition	
financial cost	0.00
hostname	
minimized icon	circle/#708090
role	

Jammer Transmitter Power

Floating Point Value: 10

Match: ○ Exact ● Substring ○ RegEx

Look in: ☑ Names ☑ Values ☑ Possible values ☑ Tags

☑ Advanced

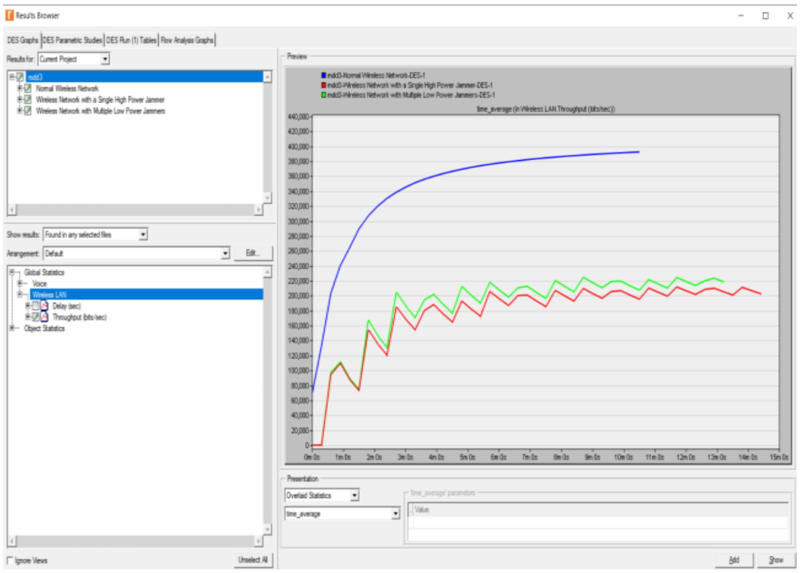
☐ Apply to selected objects

Figure 5: (Scenario 3) Network with multiple low power jammers

Scenario 3: According to our proposal, multiple low powers jammers were included instead of a single high power jammer.

These scenarios were simulated and certain parameters such as Network throughput, delay, voice jitter, packets sent and received were observed by time average graphs of the aforementioned parameters with the results of Scenario 1(without jammer) depicted by blue line, Scenario 2(with single high power jammer) depicted by red line and Scenario 3(with multiple low power jammers) depicted by green line.

We acquired the respective results as follows:


Results Browser

Results for: Current Project

☑ mdd3
☑ Normal Wireless Network
☑ Wireless Network with a Single High Power Jammer
☑ Wireless Network with Multiple Low Power Jammers

Show results: Found in any selected files

Arrangement: Default

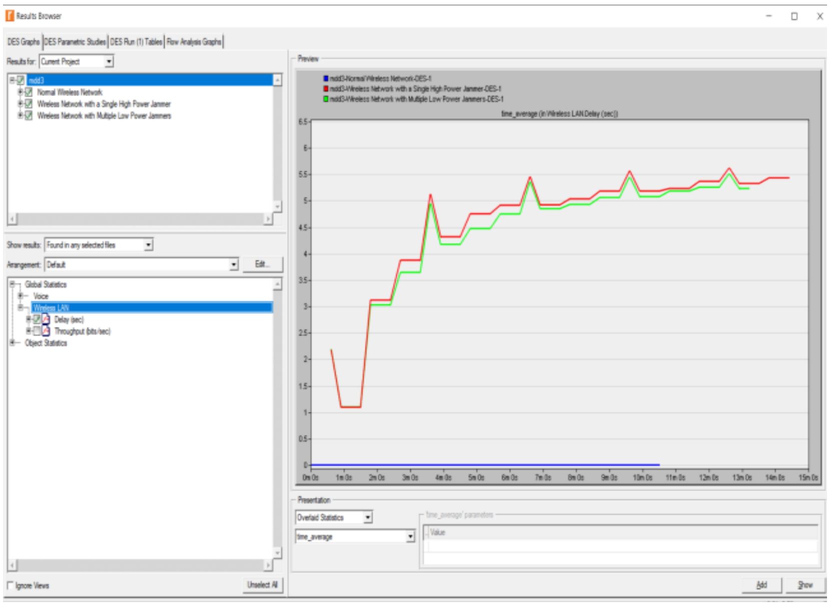
Global Statistics
Voice
Wireless LAN
☐ Delay (sec)
☑ Throughput (bits/sec)
Object Statistics

Presentation: Overlaid Statistics; time_average

☐ Ignore Views

Figure 6: Network throughput vs. Time graph

The above graph depicts Network Throughput(Y axis) vs. Simulation Time(X axis). Throughput is the efficiency of the network in bits or packets, sent and received per second. In scenario 1 a constant increase in throughput is observed. A drastic decrease and rapid fluctuation in the throughput of scenario 2 is observed. In scenario 3 we observed a similar effect on throughput of network.



Results for: Current Project

☑ mdd3
☑ Normal Wireless Network
☑ Wireless Network with a Single High Power Jammer
☑ Wireless Network with Multiple Low Power Jammers

Show results: Found in any selected files

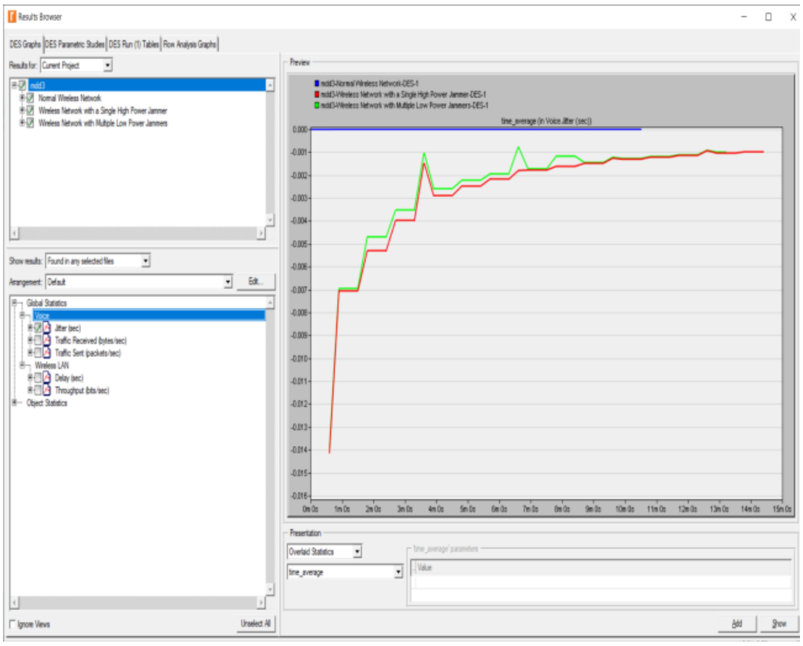
Arrangement: Default

Global Statistics
Voice
Wireless LAN
☑ Delay (sec)
□ Throughput (bits/sec)
Object Statistics

Presentation: Overlaid Statistics; time_average

Figure 7: Delay

The above graph depicts the time average Delay of the network which is the time between generation of data at source and its arrival at destination. Considering scenario 1 as an ideal network no delay is observed. While in scenario 2 and 3 we observe a significant increase in delay which is due to effect of jammers.



Results for: Current Project

☑ mdd3
☑ Normal Wireless Network
☑ Wireless Network with a Single High Power Jammer
☑ Wireless Network with Multiple Low Power Jammers

Show results: Found in any selected files

Arrangement: Default

Global Statistics
Voice
☑ Jitter (sec)
□ Traffic Received (bytes/sec)
□ Traffic Sent (packets/sec)
Wireless LAN
□ Delay (sec)
□ Throughput (bits/sec)
Object Statistics

Presentation: Overlaid Statistics; time_average

Figure 8: Voice Jitter

The above graph depicts the voice jitter which is the breakage in the flow of data in a communication network, the discontinuity to be precise. Again, considering scenario 1 as an ideal network no jitter is observed, while in scenario 2 and 3 a significant increase in jitter with time is observed due to effect of jammers.

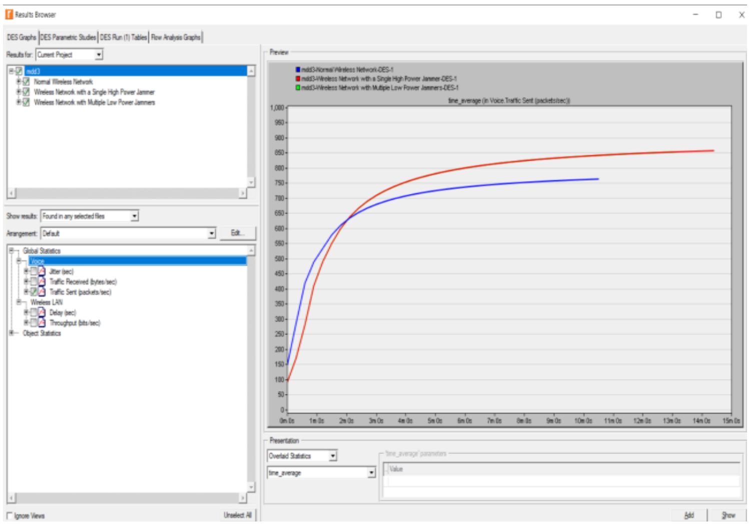

Results Browser
DES Graphs | DES Parametric Studies | DES Run (1) Tables | Flow Analysis Graphs
Results for: Current Project
mdd3
Normal Wireless Network
Wireless Network with a Single High Power Jammer
Wireless Network with Multiple Low Power Jammers
Show results: Found in any selected files
Arrangement: Default
Edit...
Global Statistics
Voice
Jitter (sec)
Traffic Received (bytes/sec)
Traffic Sent (packets/sec)
Wireless LAN
Delay (sec)
Throughput (bits/sec)
Object Statistics
Ignore Views
Unselect All
Preview
🟦 mdd3-Normal Wireless Network-DES-1
🟥 mdd3-Wireless Network with a Single High Power Jammer-DES-1
🟩 mdd3-Wireless Network with Multiple Low Power Jammers-DES-1
time_average (in Voice.Traffic Sent (packets/sec))
1,000
950
900
850
800
750
700
650
600
550
500
450
400
350
300
250
200
150
100
50
0
0m 0s
1m 0s
2m 0s
3m 0s
4m 0s
5m 0s
6m 0s
7m 0s
8m 0s
9m 0s
10m 0s
11m 0s
12m 0s
13m 0s
14m 0s
15m 0s
Presentation
Overlaid Statistics
time_average
time_average parameters
Value
Add
Show

Figure 9: Packets sent

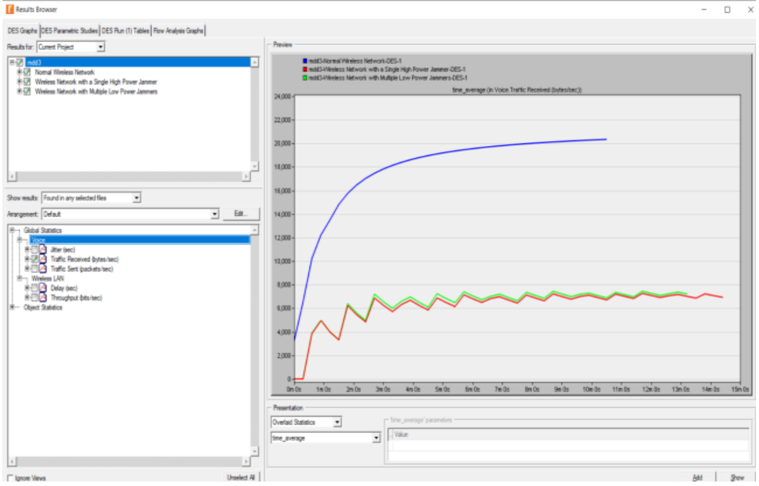

Results Browser
DES Graphs | DES Parametric Studies | DES Run (1) Tables | Flow Analysis Graphs
Results for: Current Project
mdd3
Normal Wireless Network
Wireless Network with a Single High Power Jammer
Wireless Network with Multiple Low Power Jammers
Show results: Found in any selected files
Arrangement: Default
Edit...
Global Statistics
Voice
Jitter (sec)
Traffic Received (bytes/sec)
Traffic Sent (packets/sec)
Wireless LAN
Delay (sec)
Throughput (bits/sec)
Object Statistics
Ignore Views
Unselect All
Preview
🟦 mdd3-Normal Wireless Network-DES-1
🟥 mdd3-Wireless Network with a Single High Power Jammer-DES-1
🟩 mdd3-Wireless Network with Multiple Low Power Jammers-DES-1
time_average (in Voice.Traffic Received (bytes/sec))
24,000
22,000
20,000
18,000
16,000
14,000
12,000
10,000
8,000
6,000
4,000
2,000
0
0m 0s
1m 0s
2m 0s
3m 0s
4m 0s
5m 0s
6m 0s
7m 0s
8m 0s
9m 0s
10m 0s
11m 0s
12m 0s
13m 0s
14m 0s
15m 0s
Presentation
Overlaid Statistics
time_average
time_average parameters
Value
Add
Show

Figure 10: Packets received

In this simulation software, the jammer module is considered just as a transmitter which generates/transmits data in form of packets. So, we can see that in Fig 9, the amount packets sent in scenario 1 is comparatively lower than scenario 2 and 3, thus it can be inferred that jammers are efficiently generating packets to interfere with the already existing communication flow between the nodes in scenario 1. In Fig 10, depicting the packets received per second we observe that in scenario 1, a much higher number of packets are received than other two scenarios, thus proving that the presence of jammers is decreasing the efficiency of network.

V. CONCLUSION

From our simulation we conclude that multiple low power jammers have almost a similar effect to that of a single high power jammer, thus we propose to enhance the existing MANET used in tactical environments by equipping every infantry on the field of operation with a portable manpack transceiver with individual communication, counter and counter-counter measure equipment. As a replacement for the bulky single high power jammer, each manpack to be equipped with low power jammer and a collection of such manpacks would together produce and equivalent jamming effect.

VI. FUTURE WORK.

Our future work would include carrying out simulations in much better softwares which were currently unavailable to us like CRFS RFeye[8], Deep View, SEWES, GQRX, Wireshark, RF expert, DRFMJEM considering various other parameters such as dynamic size of network topology and distance between the nodes. Further in depth study of military technologies, designing a single antenna for multiband communication along with jamming and reducing the weight of manpack transceiver (currently 6.2kgs) for increasing operational mobility and efficiency. Also there were some realistic constraints:-

1. Integration of Comms Unit and Counter Unit: The counter unit should not backfire on us that is it should not block or attenuate our own signals
2. Different scenarios such as missions conducted in plains or hilly terrains, would require different parameters to be considered such as Antenna Gain, receiver sensitivity which would thereby change distance between nodes, their mobility and velocity
3. Frequency specific jamming and counter counter-measure technique of FHSS, where only specific channels would be available.
4. Information regarding resources such as Military Standard Equipment, National frequency allocation plan allotment and military design simulators is unavailable due to secrecy
5. Distribution of transmission power of antenna: Antenna height would be reduced and optimum transmission power to be calculated after dividing the effect of a single high power jammer into multiple low power jammers

Acknowledgement

We would express our profound gratitude towards God, our parents, our Alma Mater-SRMIST and in particular Dr. Sandeepkumar P of Dept. of ECE SRMIST, who have all helped us in ideation and completion of this proposal.

References

[1]. S. Al-Shehri and P. Loskot, “Enhancing Reliability of Tactical MANETs by Improving Routing Decisions,” *Journal of Low Power Electronics and Applications*, vol. 8, no. 4, p. 49, Nov. 2018.

[2]. C. E. Fossa and T. G. Macdonald, "Internetworking tactical MANETs," *2010 –MILCOM 2010 MILITARY COMMUNICATIONS CONFERENCE*, San Jose, CA, 2010, pp. 611-616, doi: 10.1109/MILCOM.2010.5680456.

[3]. Jahnke, Marko & Wenzel, Alexander & Klein, Gabriel & Aschenbruck, Nils & Gerhards-Padilla, Elmar & Ebinger, Peter & Karsch, Stefan. (2008). “MITE – MANET Intrusion Detection for Tactical Environments”. *Conference: NATO/RTO Research Symposium on Information Assurance for Emerging and Future Military Systems (RSY IST-076*

[4]. H. Zhao, "Simulation of Barrage-Type Jamming for Synthetic Aperture Radars," *2008 ISECS International Colloquium on Computing, Communication, Control, and Management, Guangzhou*, 2008, pp. 462-465, doi: 10.1109/CCCM.2008.96.

[5]. Lalitha, V. (2013). “The Impact of Transmission Power on the Performance of MANET Routing Protocols.*” IOSR Journal of Engineering*. 03. 34-41. 10.9790/3021-03233441.

[6]. Mishra, V. & S. Jangale. “Analysis and comparison of different network simulators.” (2014*). International Journal of Application or Innovation in Engineering & Management (IJAIEM*)

[7]. Pawan Popli & Paru Raj. (2016). “Securing MANET by Eliminating Jamming Attack through Mechanism.” *International Journal of Science, Engineering and Technology Research (IJSETR)* Volume 5, Issue 9

[8]. R. F. Mofrad and R. A. Sadeghzadeh, "Scenario modeling and simulation for performance prediction of a modern radar in electronics warfare environment," *11-th INTERNATIONAL RADAR SYMPOSIUM, Vilnius*, 2010, pp. 1-5.

[9]. G. Klein, H. Rogge, F. Schneider, J. Toelle, M. Jahnke and S. Karsch, "Response Initiation in Distributed Intrusion Response Systems for Tactical MANETs," *2010 European Conference on Computer Network Defense, Berlin,* 2010, pp. 55-62, doi: 10.1109/EC2ND.2010.11

[10]. Abdalla I. Abrwais, Asmahan M. Khaled, Abdanaser A. & Alsousi,Jalal Sarar, “Influence of Jammers on GSM Mobile Network”. *International Journal of Engineering Research & Technology (IJERT)* Vol. 4 Issue 08, August-2015

[11]. Tutika, Chetan & Kumar, A. & Charan, V. & Sekar, Ramya. (2016). “Design of automated dual B and 4G jammer using MATLAB Simulink”. *Indian Journal of Science and Technology*. 9. 10.17485/ijst/2016/v9i37/95125.

[12]. Starovoytova, Diana. (2016). “Design and Testing of a Mobile-Phone-Jammer”. *American Journal of Engineering Research (AJER*). Volume-5, Issue-2, pp-71-76.

Sanyatjeet Pawde, Aditya Garg "Jampack: An Enhancement in Design of Tactical Manet And Manpack Transceiver." *IOSR Journal of Electronics and Communication Engineering (IOSR-JECE)* 15(6), (2020): 36-43.