OPNET PROJECT INTERIM REPORT

EFFECTIVENESS OF RTS/CTS ON JAMMER ENABLED 802.11n NETWORKS AND MEANS OF INTELLIGENT JAMMING IN 802.11n

BHARATH VENKATESH
[001037220]
TRUPTESH M N
[200021946]

OBJECTIVE:

- Implement RTS/CTS enabled 802.11n Networks.
- Analyze appropriate power levels and packet size which introduces hidden nodes in the network and demonstrate the usefulness of RTS/CTS in 802.11n.
- Introduce a Single Band/Pulse Jammer in the network to analyze the effectiveness of Jammer in disrupting the network.
- Verify if the RTS/CTS mechanism can counter the effects of Jammer to a considerable level in 802.11n
- Extend the model further to design intelligent jammers which can disrupt the network with minimal chances of them being detected.

PROJECT DESCRIPTION

Request to Send/Clear to Send mechanism has been designed to resolve the hidden node problem that arises in wireless networks. Several papers have been published that demonstrate the effectiveness of RTS/CTS in 802.11 a/b/g networks. One of our basic scenario is to extend this model to 802.11n networks and verify if RTS/CTS is equally effective. Since the transmitting data rate changes between these nodes, one of the primary requirements to accomplish extension to 802.11n networks is to find appropriate power levels and packet sizes at which nodes become hidden in the network and toggling these values see the deterioration in the throughput. Once that is done, we verify if RTS/CTS mechanism can counter this problem effectively.

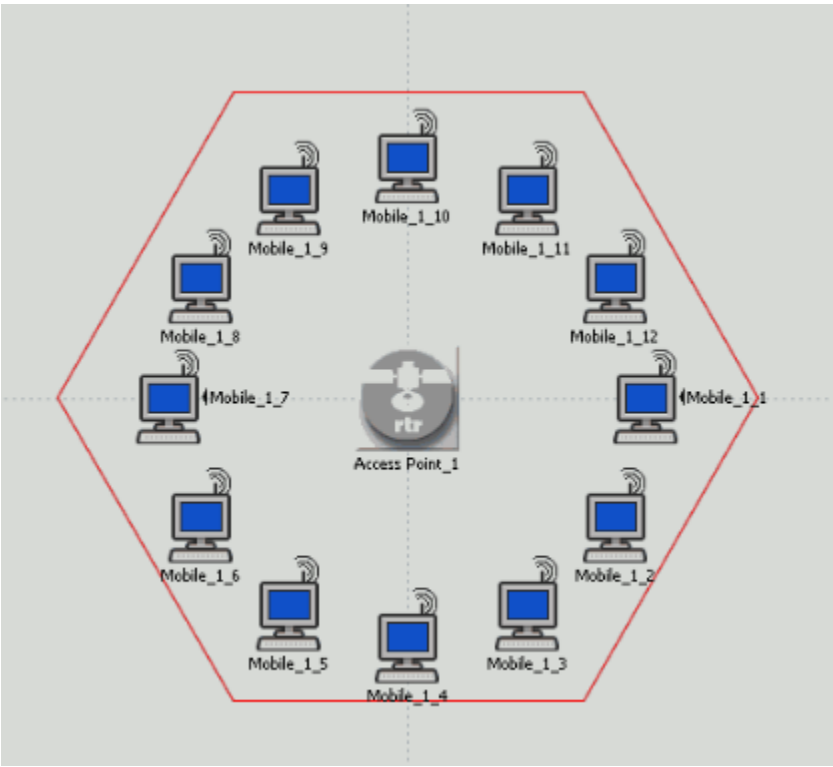
Once a design model of 802.11n with RTS/CTS is ready, the next primary aspect of this project is to see how effective a jammer works in disrupting this network communication. To accomplish this we introduce a single band jamming node in the network. We introduce jamming nodes in both RTS/CTS enabled and RTS/CTS disabled scenarios and see if the impact of the jammer remains comparable in both the scenarios or if the existence of RTS/CTS causes any considerable difference.

Although the jammer we have implemented succeeds in disrupting the network to a considerable extent, the problem with these jammers is that they are very easily detectable and several mechanisms have already been designed to detect and correct these jammer disruptions. We thus plan to implement intelligent jammers using 802.11e nodes in the network wherein we will prioritize certain type of traffic over other type thus causing some nodes in the network to internally jam other nodes from transmitting. This method of intelligent jamming can be highly effective in loading the network to the maximum extent yet not allowing other nodes to transmit. They are also very hard to detect as it becomes difficult to decipher a misbehaving node from a jammer node. [2] successfully demonstrates the above explained scenario for 802.11b nodes and this been extended to demonstrate the effects for 802.11g nodes in [3]. Our plan is extend this scenario on 802.11n nodes to see if the same effects can be replicated or if 802.11n causes a considerable change in the observations.

IMPLEMENTATION

Basic Network Design

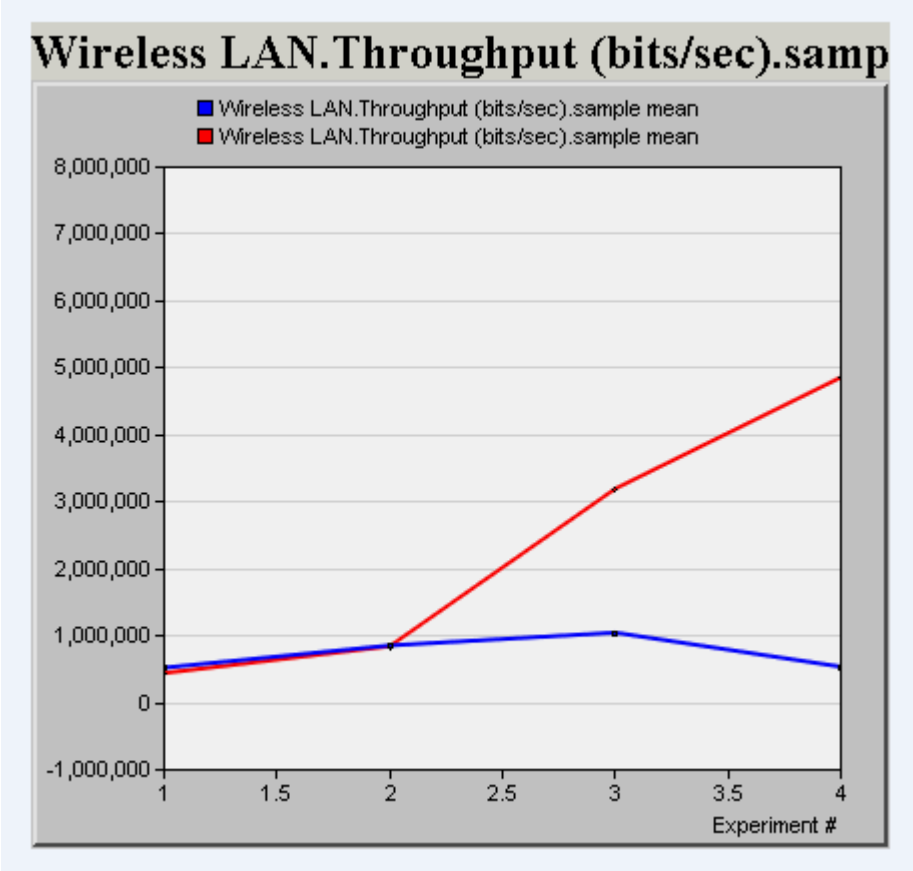
The basic network design has a network of 12 nodes that are connected to an Access Point in the form of a hexagon.



SCENARIO 1: Impact of RTS/CTS for 802.11g Networks

- The 1332 Lab2 scenario was a model that described the impact of RTS/CTS in improving the network performance for 802.11g network. We first started by implementing this scenario.

  We measure the sample mean Throughput for both the scenarios.
  The results were obtained as follows



Blue – Without RTS/CTS
Red – With RTS/CTS Enabled

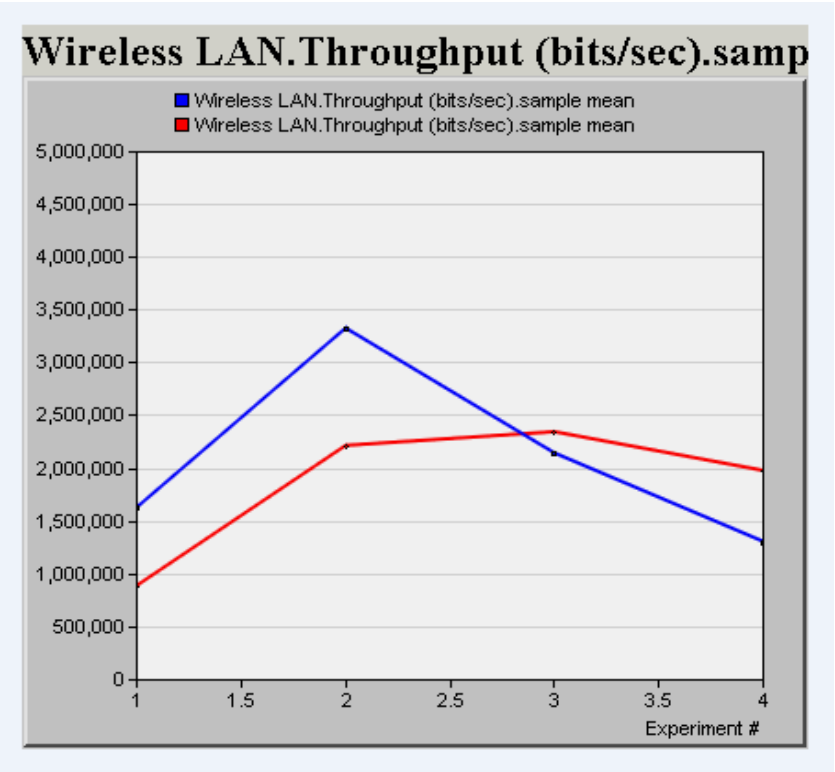
Analysis:

When there exists hidden nodes in the network we can observe that with RTS/CTS disabled, the throughput reduces as the packet size increases. By enabling the RTS/CTS we resolve the hidden node problem and thus the throughput increases with the increase in Packet Size.

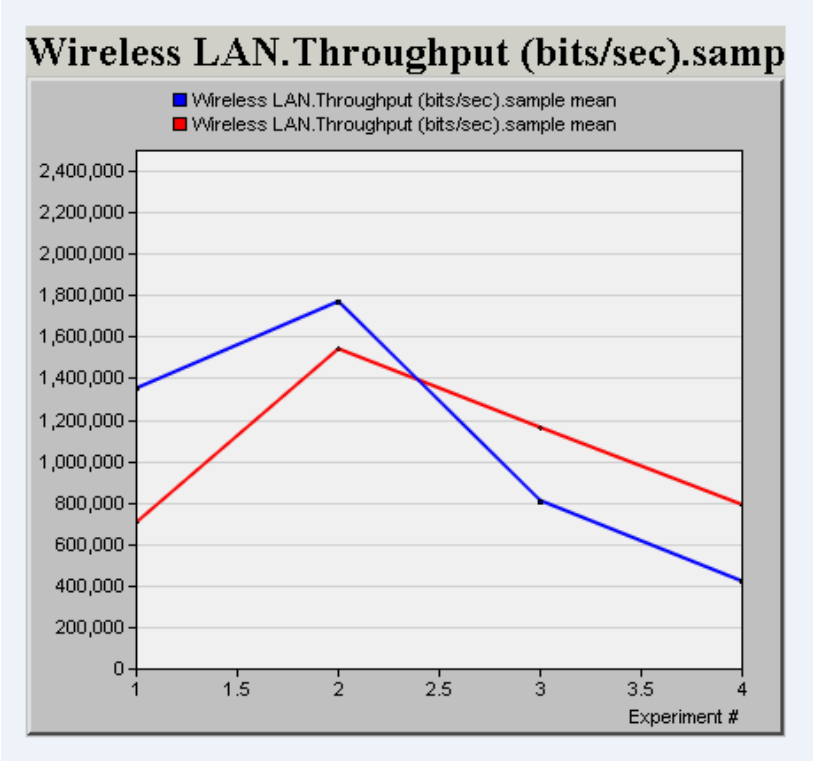
Scenario 2: Extend RTS/CTS impact scenario for 802.11n Networks

In this scenario we extend the above demonstrated scenario for 802.11n networks. To implement this we initially tried by keeping all other parameters same and changing the node and AP to 802.11n operating at 2.4Ghz with Base Data rate of 26Mbps and Max Data Rate of 240 Mbps. We observed that the throughput dropped to 0 in that case. A possible explanation to that is that when we changed the nodes to 802.11n with higher data rate it would have resulted in a higher frequency which in turn decreases the wavelength. We know that loss in wireless medium is inversely proportional to wavelength and thus it would result in the observed scenario. We varied the packet size and power parameters of the nodes and AP to deduce a packet size and power of transmission for which we could see a tangible impact for RTS/CTS. We introduced four hidden nodes in the network [Node 6,7,8 and 9] by reducing their power of transmission to 0.012W. The rest of the nodes and the AP were

transmitting at 0.1W. We ran a parameterized run with 4 packet sizes 100,500, 1000 and 1500 respectively. The results obtained were as follows.



Run2: Same parameters as previous scenario but the Channel being specifically set to a random channel[Channel 3]



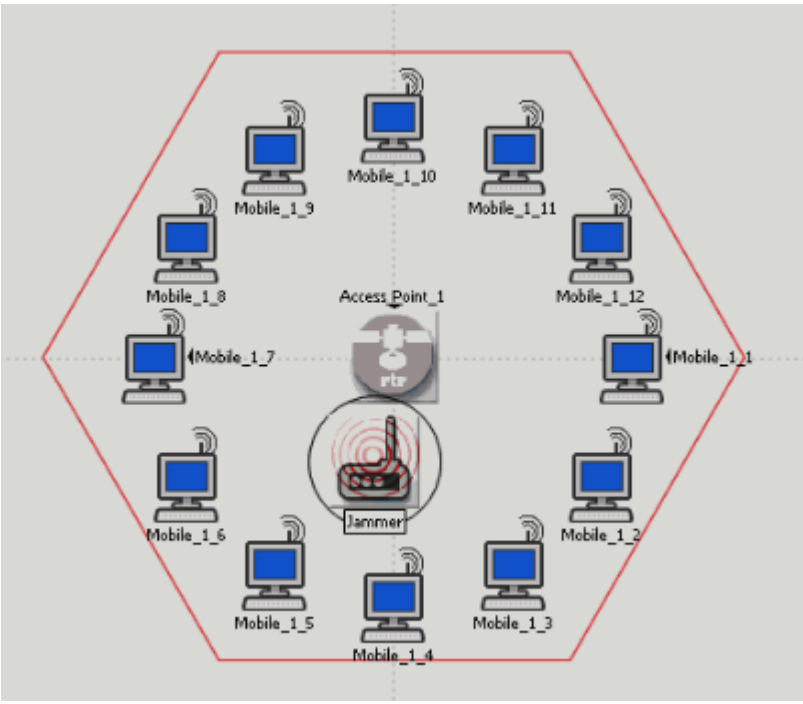
Blue – Without RTS/CTS
Red – With RTS/CTS Enabled

Analysis:

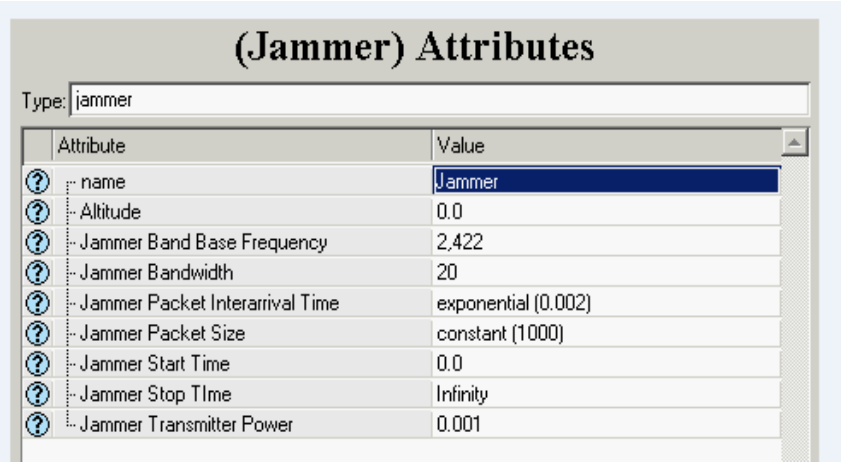
At the initial stages I.e when packet size is less, we see that the throughput for RTS/CTS disabled scenario is better than that of the enabled scenario. This is because, when small packets are traveling in the network, the overhead of having a RTS/CTS frame before the actual frame is considerably higher than the problem of the hidden nodes existing in the network. However for higher packet sizes we see that RTS/CTS is effective in increasing the throughput thus indicating that RTS/CTS enable does successfully solve the hidden node problem in 802.11n network.

Scenario 3: Impact of Single Band Jammer in a 802.11n Network with RTS/CTS disabled and enabled

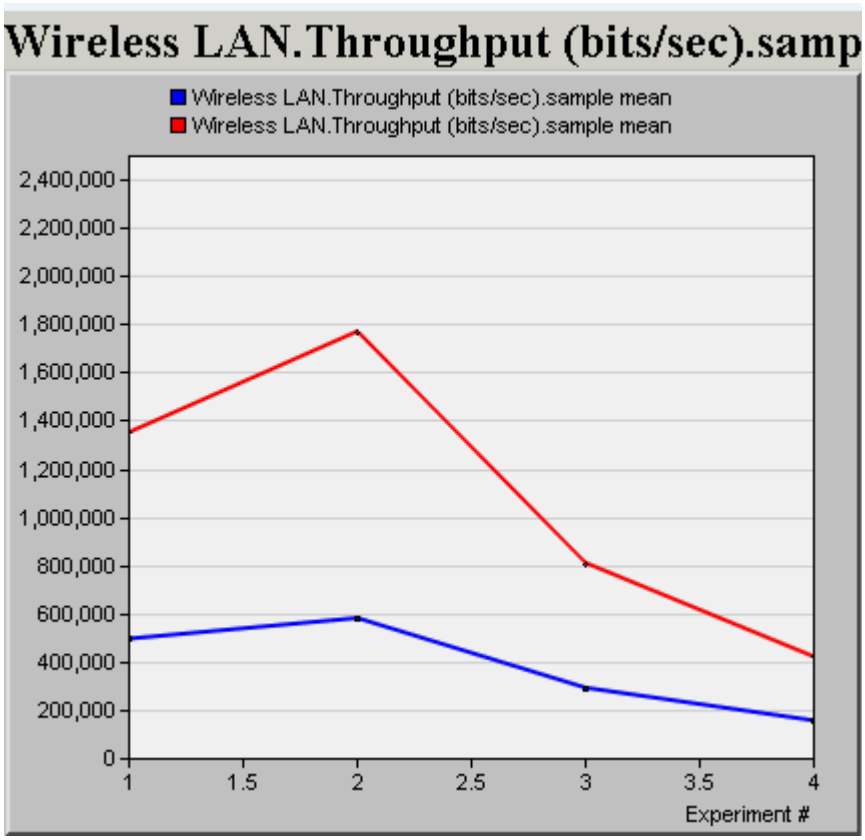
In this scenario we extended the 3 channel scenario and further introduced a single band jammer. The network is as shown below.



The Jammer is configured with its attributes as shown below.



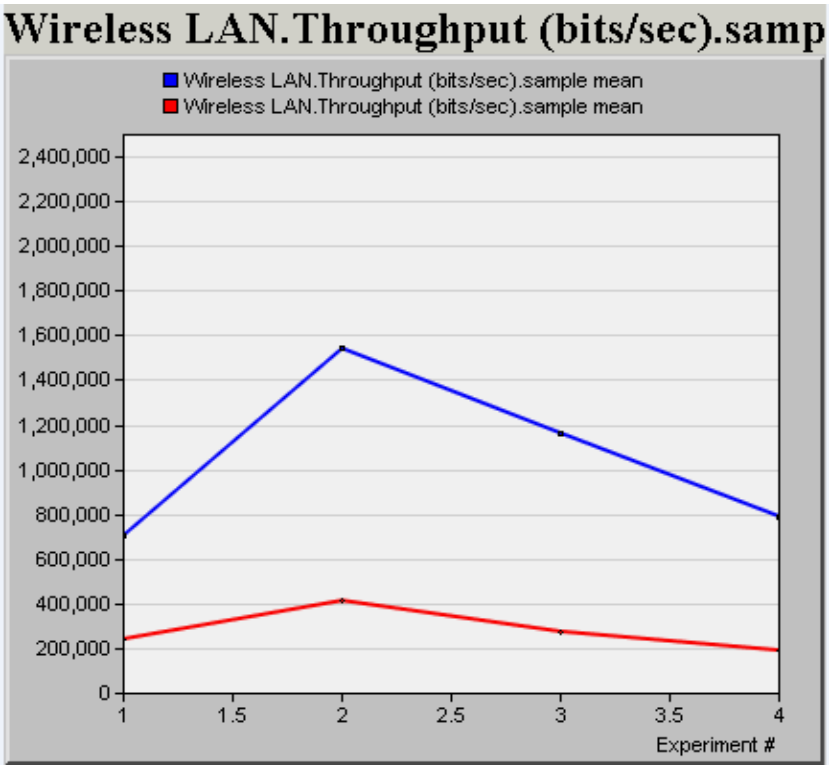
We observed an output as follows.



Red – RTS/CTS Disabled 802.11n Network
Blue – RTS/CTS Disabled 802.11n Network with Jamming Node

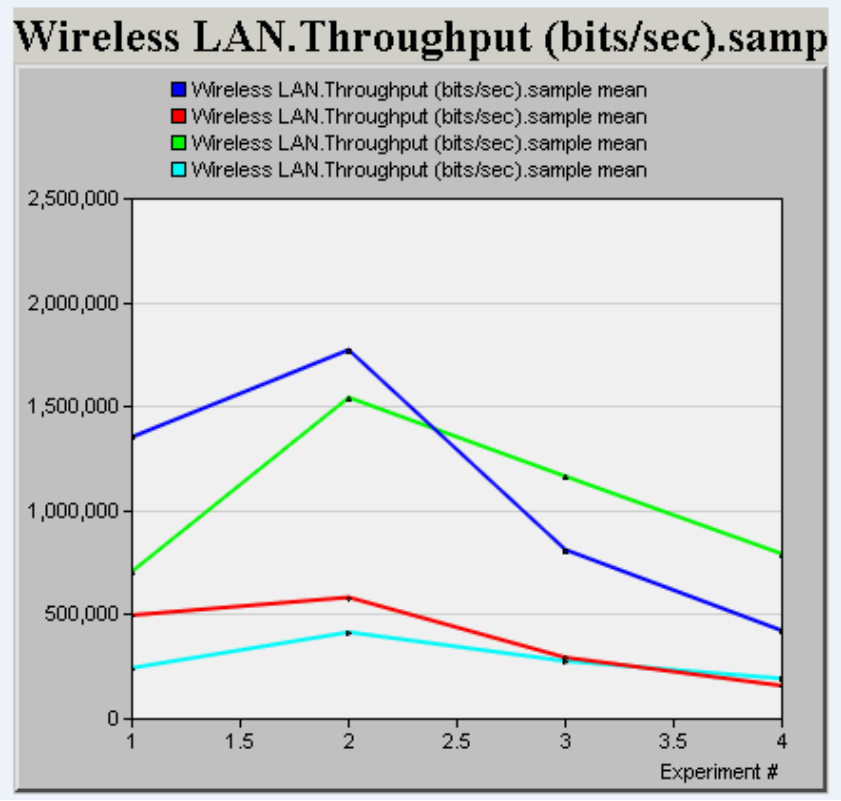
A similar result was obtained when a jammer was introduced to a RTS/CTS enabled 802.11n Network.

The result is as shown below



Blue – RTS/CTS Enabled 802.11n Network
Red – RTS/CTS Enabled 802.11n Network with Jamming Node

When all these four stage graphs were interlaced then throughput graph looks as follows



Red – RTS/CTS disabled with Jammer
Cyan – RTS/CTS enabled with Jammer
Blue- RTS/CTS disabled without Jammer
Green – RTS/CTS enabled without Jammer

Analysis:

We see that the jammer was very effective in disrupting the network both with and without RTS/CTS. Although the RTS/CTS enabled network fared well in comparison to the disabled network there still exists comparable disruptions at both the networks on introduction of a Jammer.

FUTURE IMPLEMENTATIONS:

- We have verified the effect of Jamming on 802.11n with a Single Band Jammer. We plan to replace these Jammers with Pulsed Jammers to see what impact the type of Jammers will have on the network performance.
- We further plan to change the type of traffic to VOIP to see if type of traffic will have an impact on the Jammer effectiveness.
- Although these Jammers are successful in disrupting the network, these networks are easily detectable and thus as described in the Project Description, our key objective is to to replace this Jammer with some intelligent Jamming techniques like priority Jamming to measure their effectiveness on a 802.11n network.

DELINEATION OF DUTIES

Truptesh MN: Study of research papers regarding 802.11n protocol and jamming and anti-jamming techniques.
Bharath Venkatesh: Implementation of design models in OPNET and evaluation of results.

OPNET MODELS:

1332 Lab2 scenario was used to implement a 802.11g network with RTS/CTS threshold.
1504 Lab 2 was used to know about how jamming node can be used to create interference.

REFERENCES:

- Shaiful Alam Chowdhury, Mohamamd Tauhldul lslam, Fariha Tasmin Jaigirdar, Md. Rokan Uddin Faruqui, Shahid AI Noor, “Performance study and simulation analysis of CSMA and IEEE 802.11 in Wireless Sensor Networks and limitations of IEEE 802.11”, International Conference on Computer and Information Technology,December 2009
- Acharya, M., and D. Thuente, “Intelligent Jamming Attacks, Counterattacks and (Counter)2 Attacks in 802.11b Wireless Networks”,OPNETWORK 2005, September 2005.
- Thuente D.J, Newlin Benjamin, Acharya M, “Jamming Vulnerabilites in 802.11e” , Military Conmmunications Conference 2007
- D.J. Thuente and M. Acharya “Intelligent Jamming in Wireless Networks with Applications to 802.11b and Other Networks,” in IEEE MILCOM 2006.
- Tiang Fu, “Modeling and Simulation of Jamming attacks in WLAN”,Thesis Work, Department of Technology Systems, East Carolina University, April 2012.