A Machine Learning Approach for Protecting Wireless Networks Against Virtual Jamming Based Denial of Service (DoS) Attacks.

Presented by..

Yeaseen Arafat

Authors..

Yeaseen Arafat

Kazi Samin Yeaser

Arnab Dasgupta

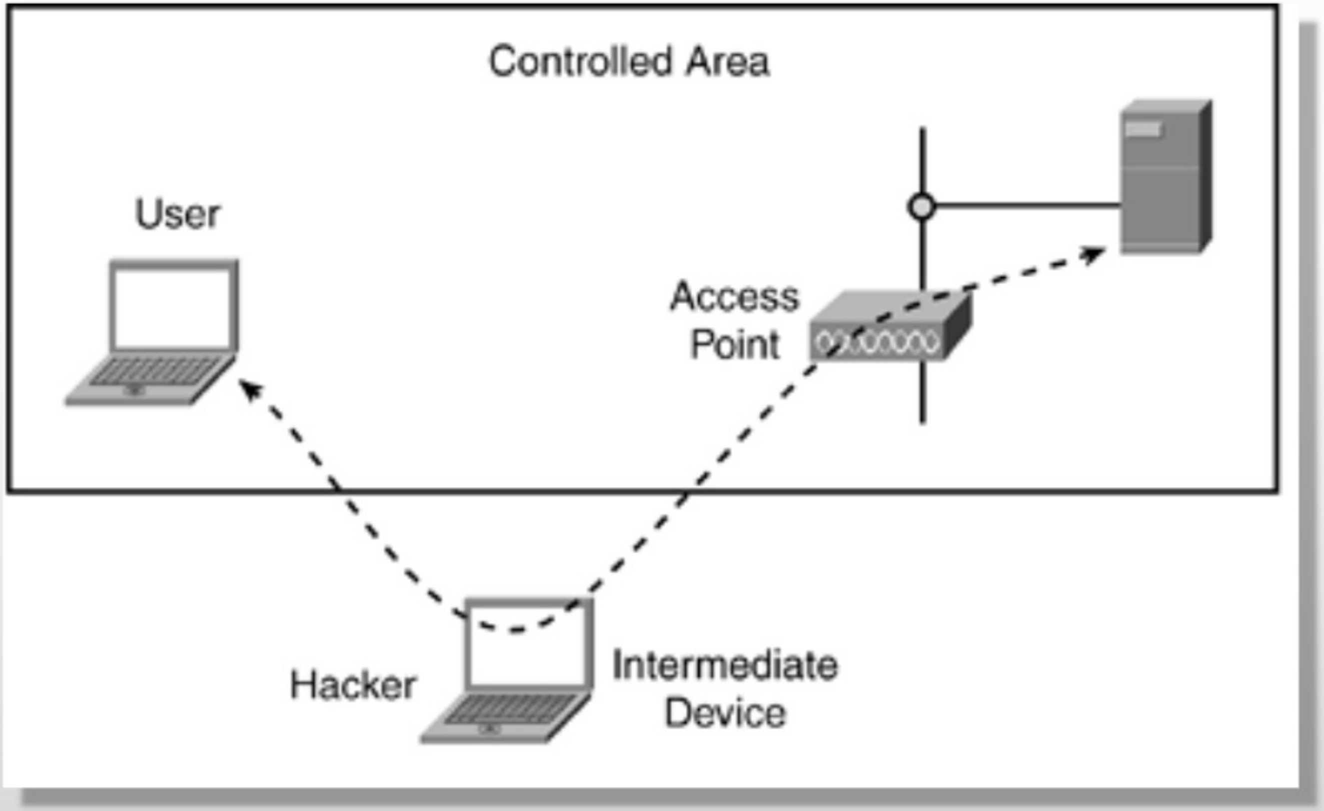
Dr. A.K.M. Ashikur Rahman

Welcome to Networking Security Inc!

DoS Attack

Virtual Jamming

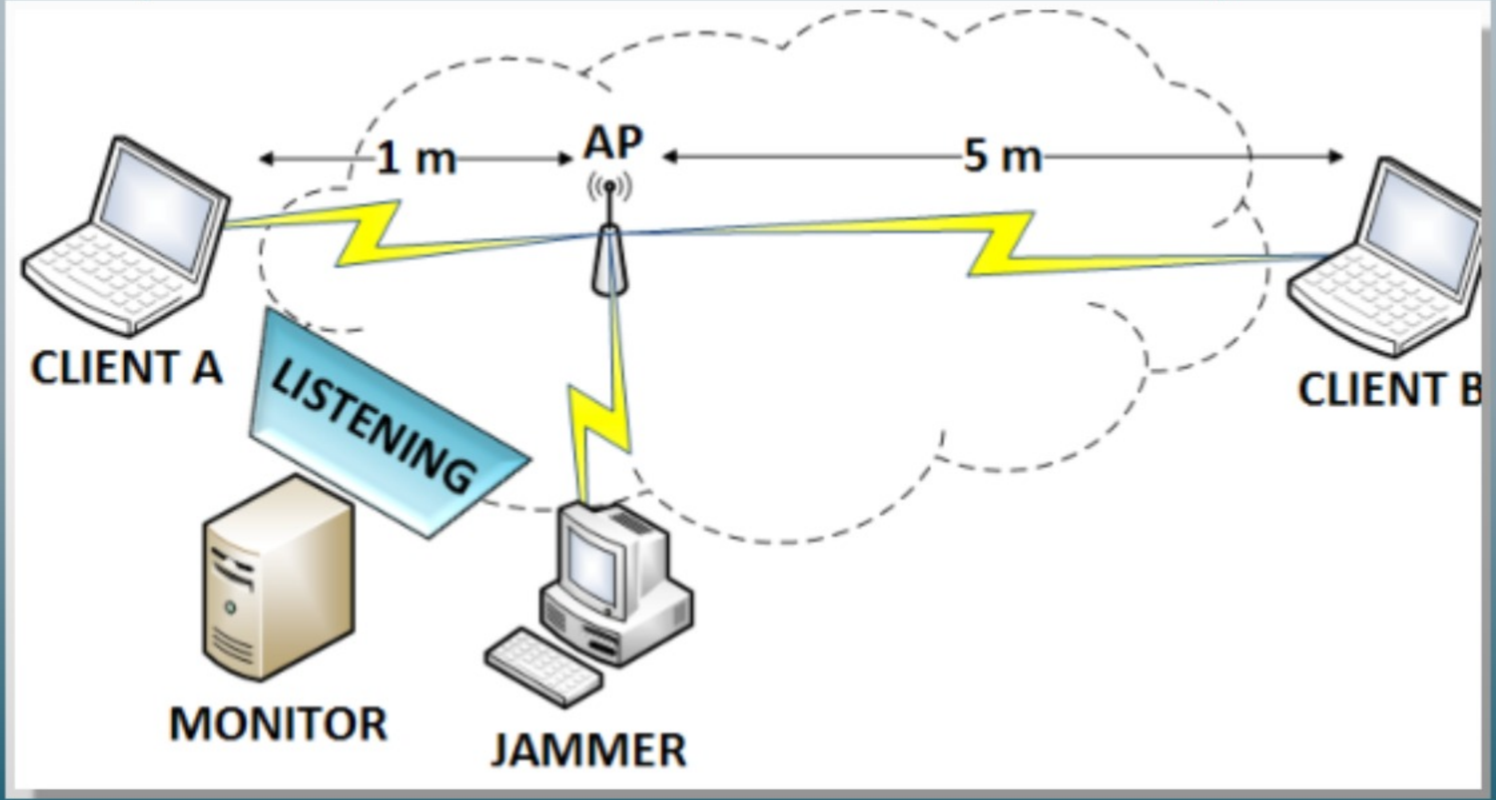
DoS : Denial of Service Attack..



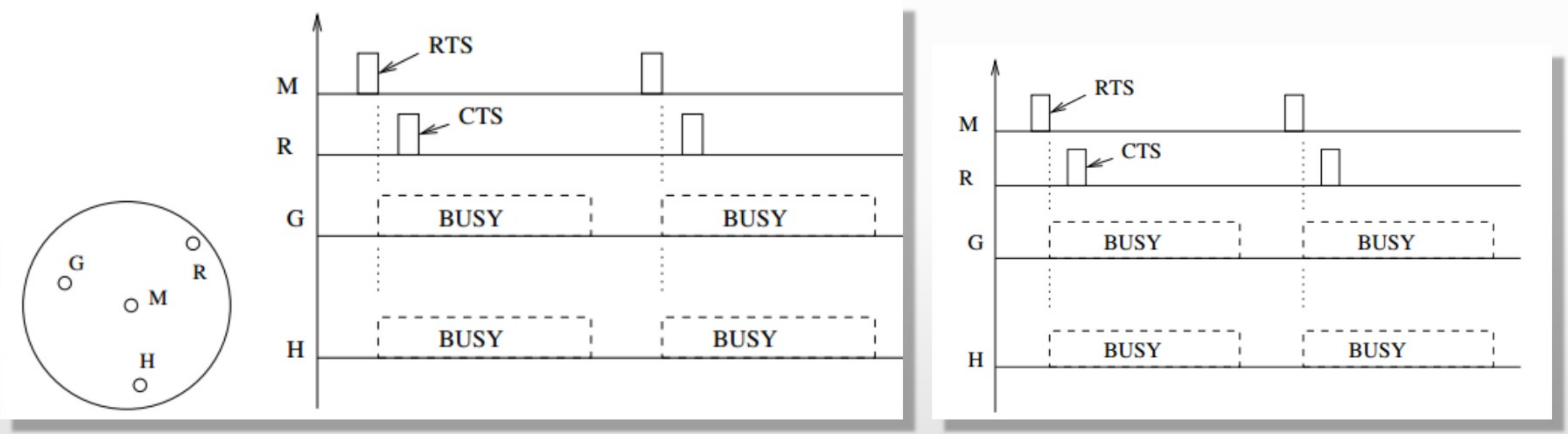
An action impairs authorized use of services by exhausting the resources.

Virtual Jamming..

What's going on here!!!

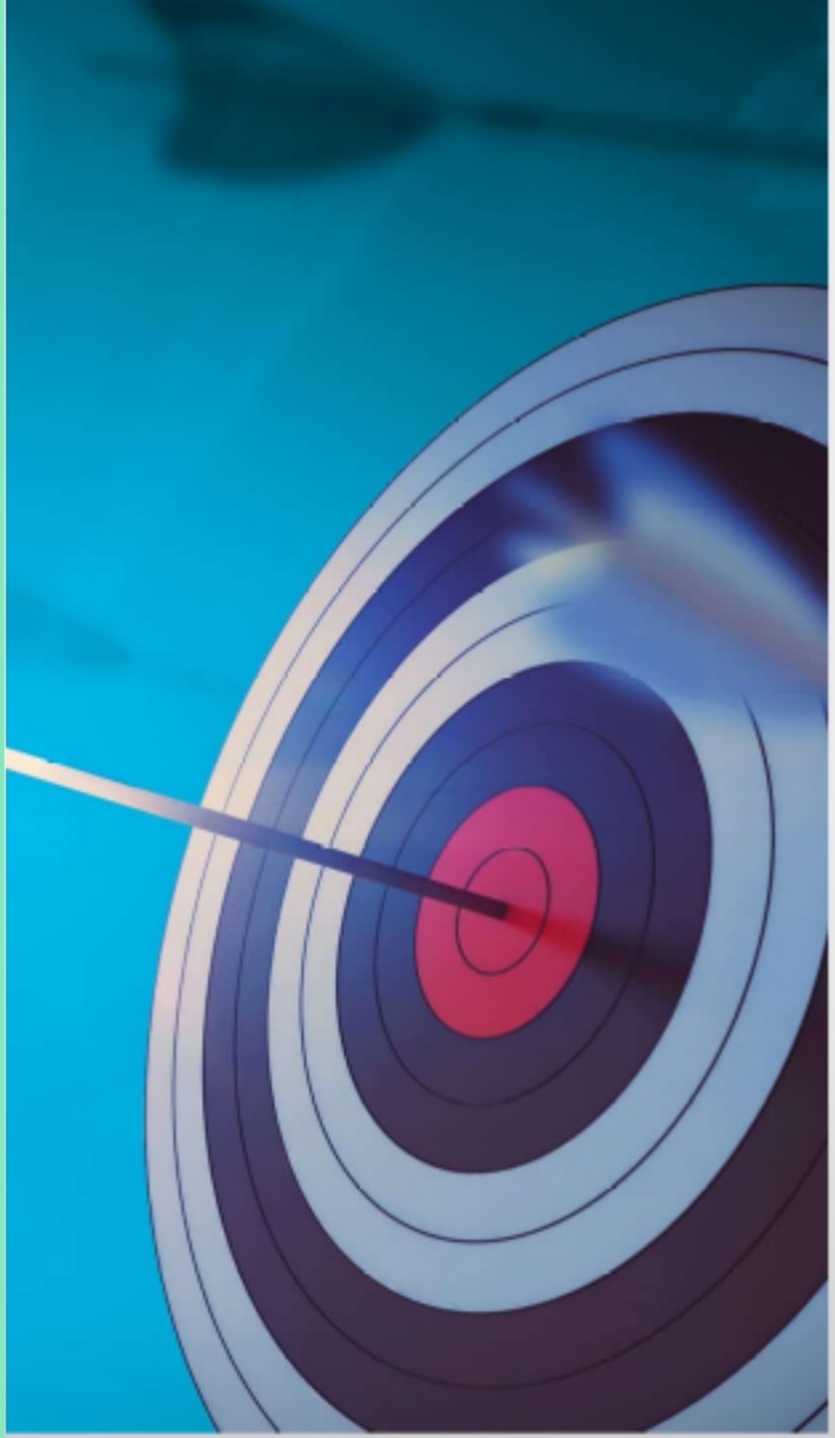


Virtual Jamming Illustration..



a. b. c.

Figure: a) Scenario b) RTS-CTS-DATA-ACK handshake c) Virtual Jamming



- Detection of Malicious Nodes using ML
- Isolation of identified malicious nodes

Previous work..

RTS validation. [1]

Random RTS validation. [2]

RTS validation [1]..

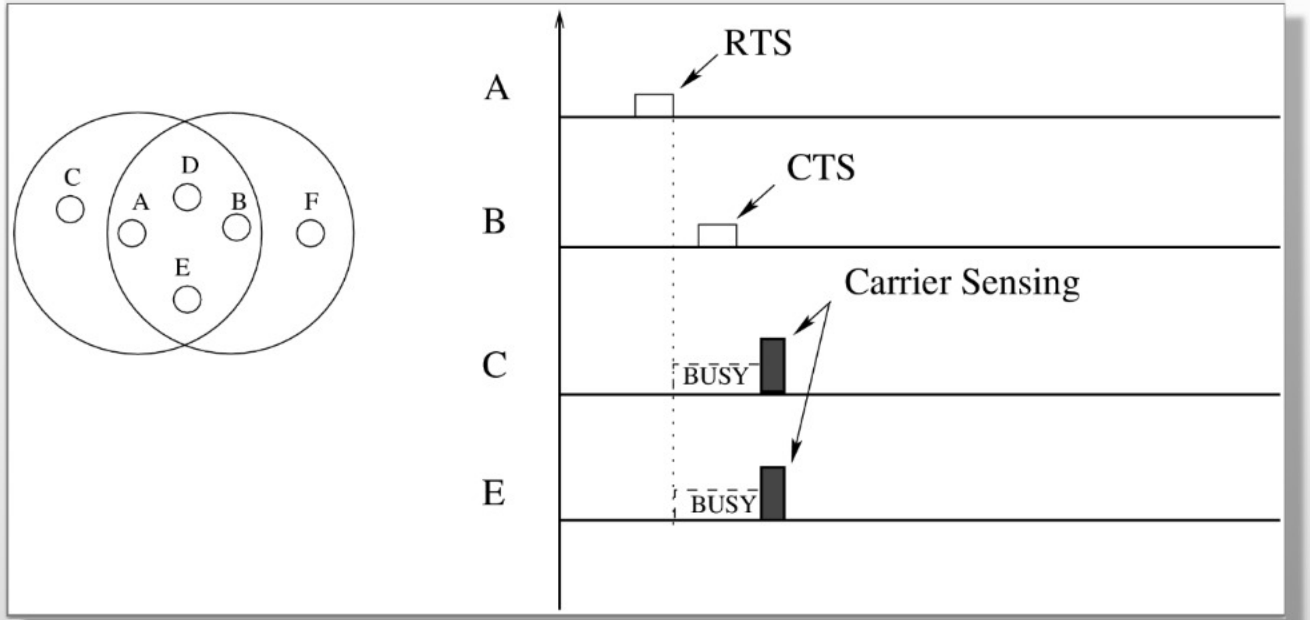


Figure: RTS Validation Illustration.

- RTS packets within a limited trust
- Carrier sensing.
- Unblocks blocked node if the transmission doesn't occur.

Drawbacks..

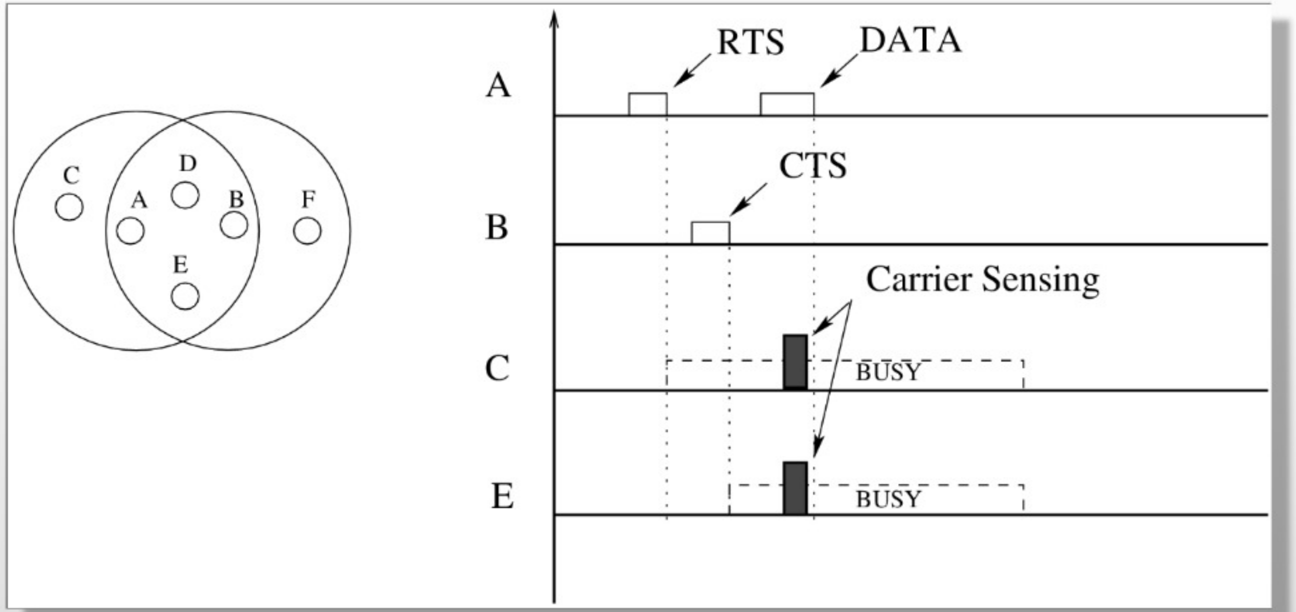


Figure: False Negative Case.

- Attacker may be concern about the prevention mechanism.
- Sends a short dummy data packet.
- Leads to false negative issue.

Random RTS Validation [2]..

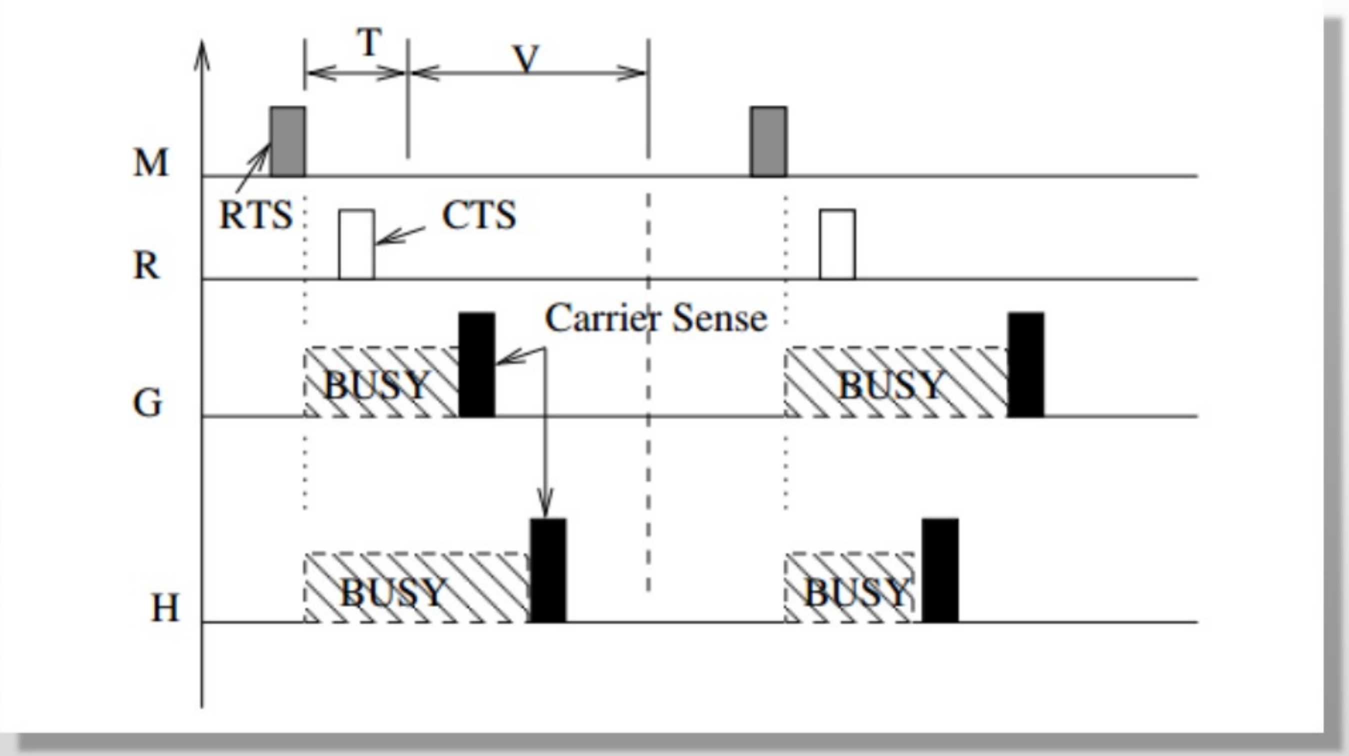


Figure: Random RTS Validation Illustration.

- Equal-sized slots of data transmission time.
- Random Carrier Sensing

STUDIED TOPOLOGY..

Data transmission flows are 1->5, 2->6, 3->7 and 4->8.

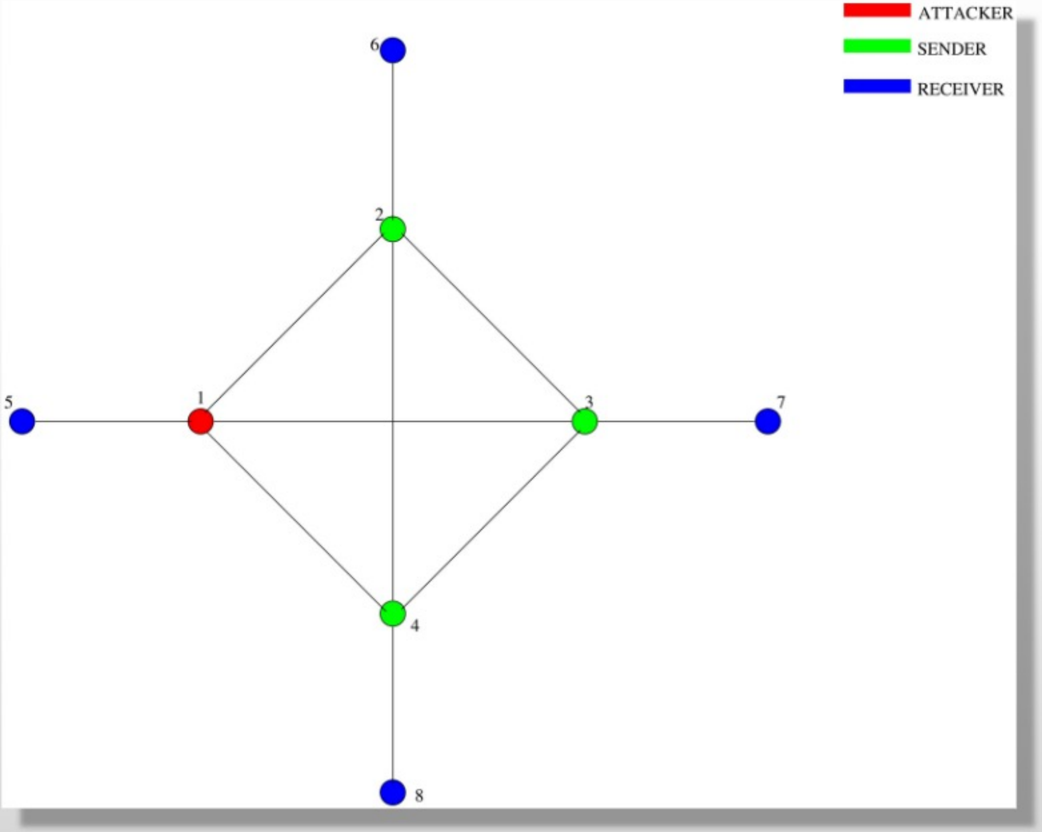


Figure: Topology.

Effect of DoS Attack

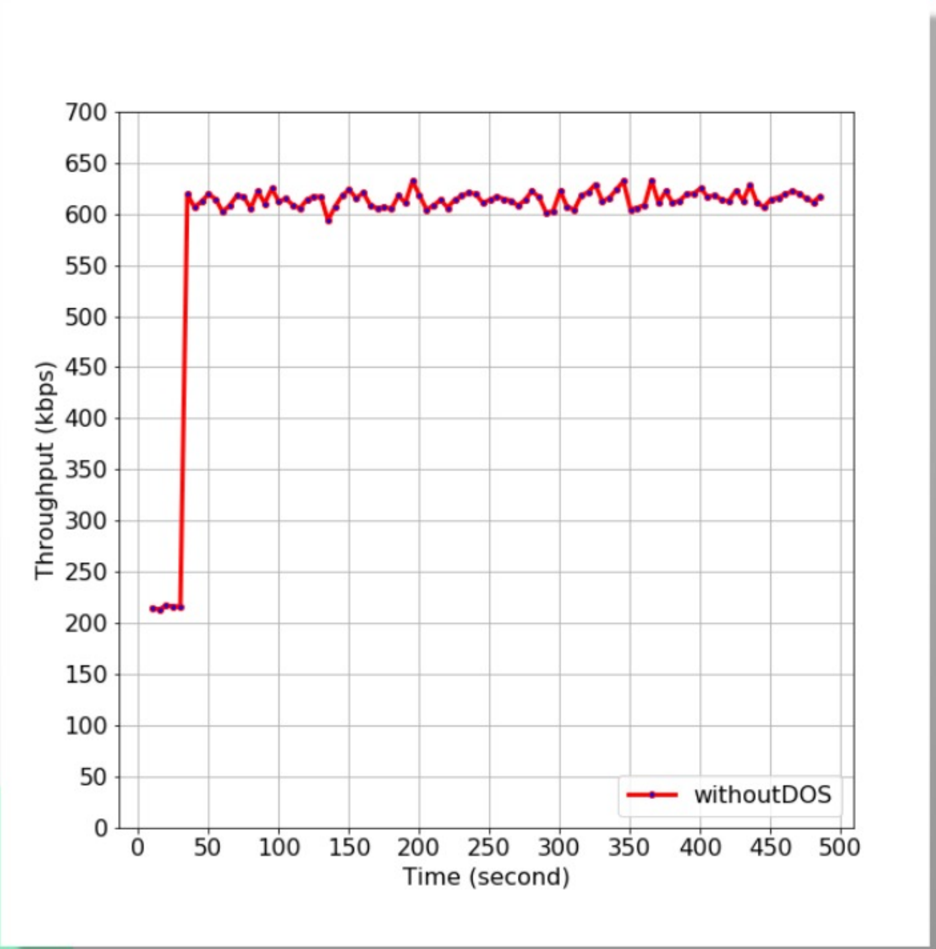


Figure 1: Scenario with No Jamming.

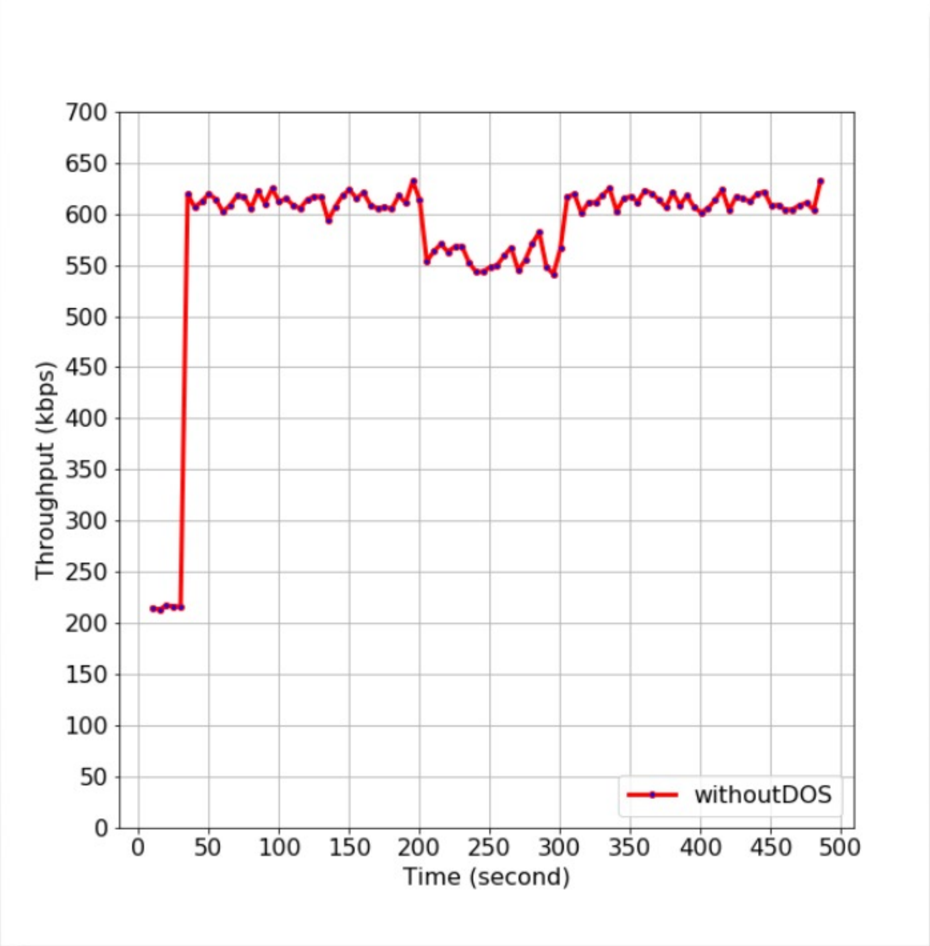


Figure 2: Scenario with Jamming.

Effect of Random RTS validation..

- Improves Throughput curve by some degree.

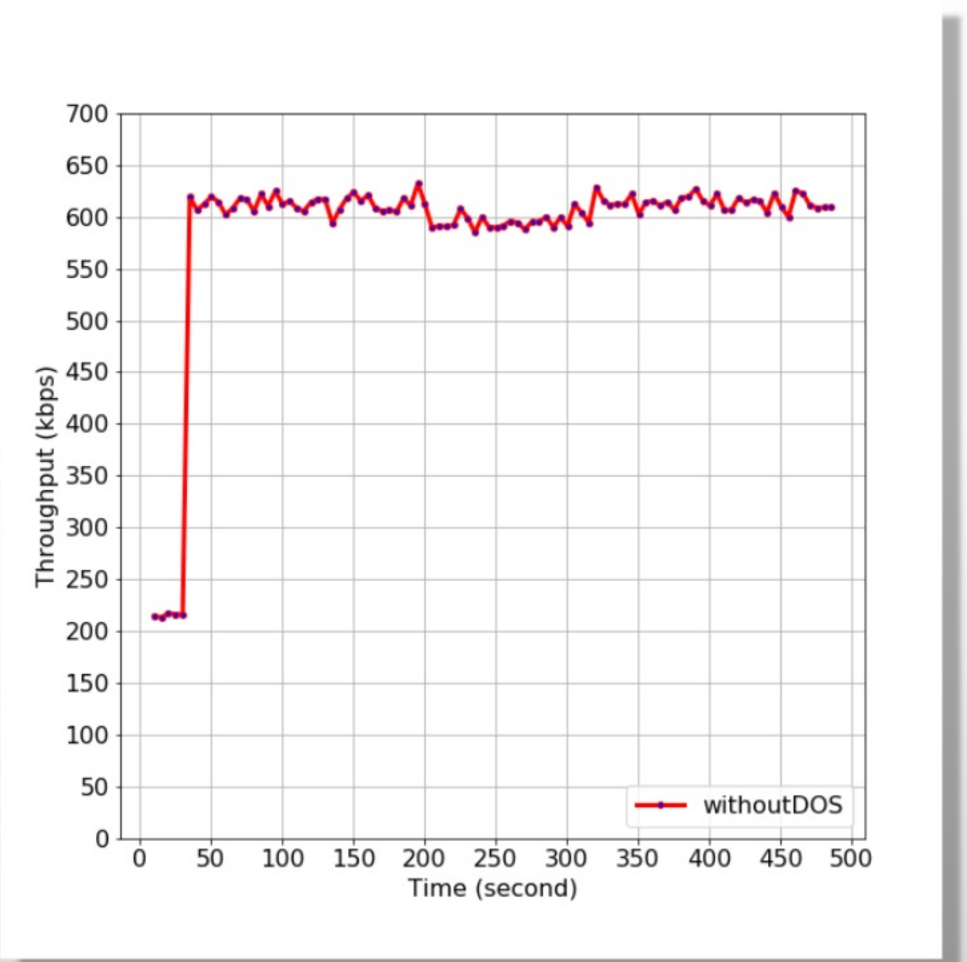
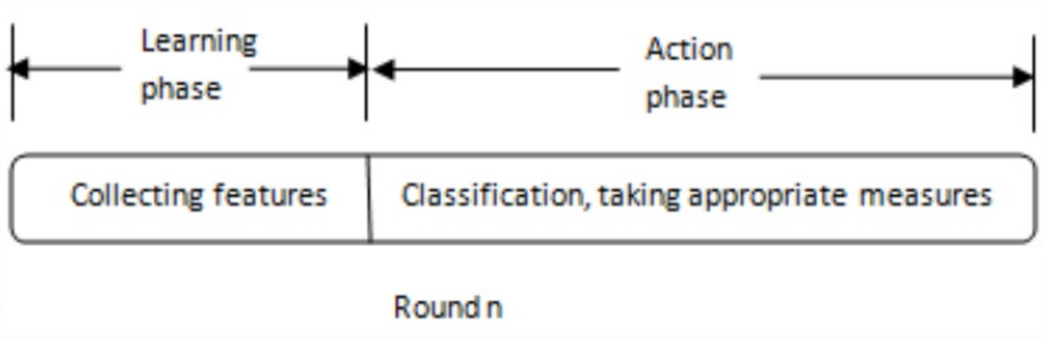


Figure: Scenario with Jamming and Random RTS Validation.

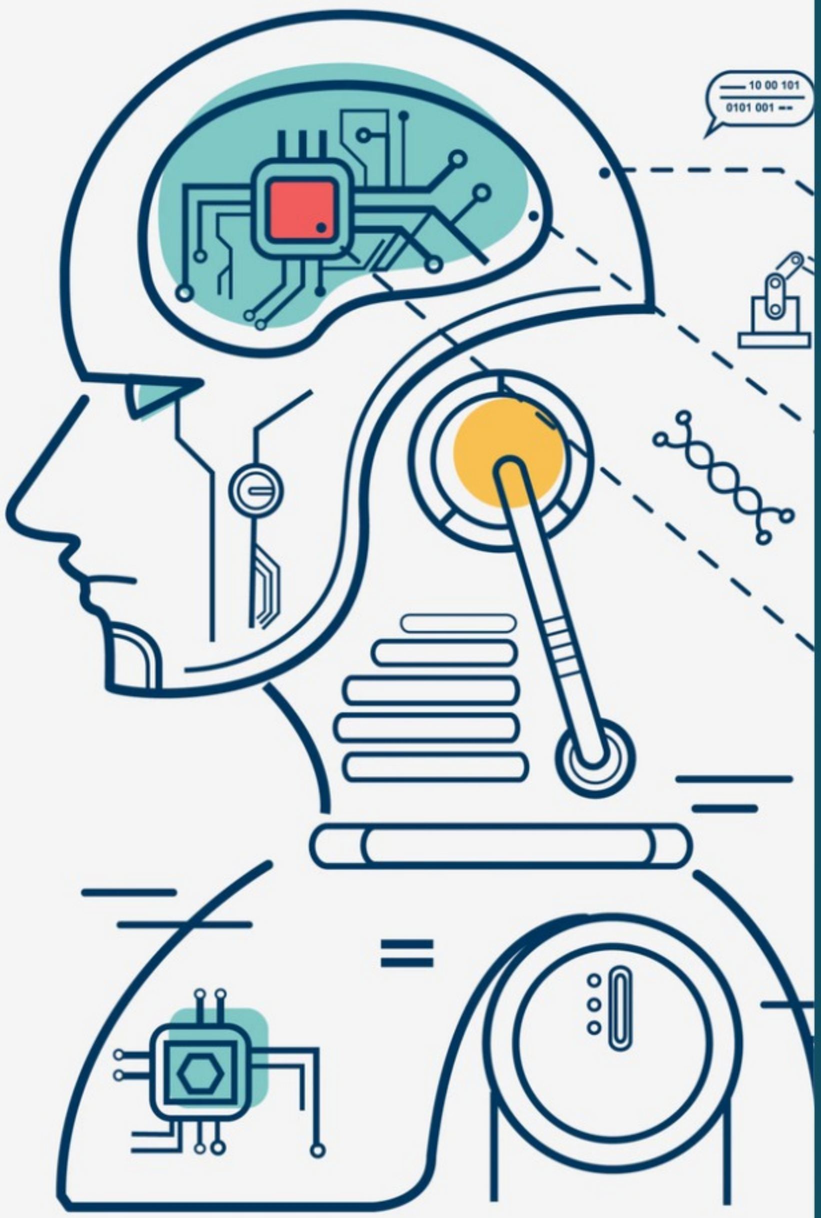
Methodology..

- Machine Learning Approach
- Learning Phase
- Action Phase

Machine Learning Approach!



- Runs periodically.
- Each Period Consists of 2 phases.
- Learning phase and Action Phase.
- Runs learning phase for a short time.
- After learning phase, action phase runs.
- Repeats two phases one after another.



Machine Learning Approach!

Learning Phase:

- Performs random RTS validation.
- Takes statistical data about neighboring nodes as different features.
- Average throughput recovery becomes 50% or so.

Action Phase:

- Classifies all the senders either Malicious or Well-behaved node.
- Runs random RTS validation for Well-behaved nodes.
- Ignores RTS packet from malicious nodes.
- Statistical data about neighboring nodes as different features are also collected.
- Average throughput recovery becomes approximately 100%.

Novelty..

- In Random RTS Validation on average half of the time can't be recovered.
- About 50% resources are wasted.
- In our method 50% resources of the learning phase will be wasted.
- Total resource waste percentage can be decreased by maintaining optimized ratio of LAR.
- In terms of backward compatibility, our model makes no change in IEEE 802.11 protocol.

Selected Features..

Moving average of IRR

Deviation of Moving Average of IRR.

Moving Average of Inter Arrival Time of RTS packet.

Moving Average of IRR..

- Calculated in both learning phase and Action phases.

- Calculate the Moving Average from data collected from Previous Period, Last Action Phase and Previous learning phase.

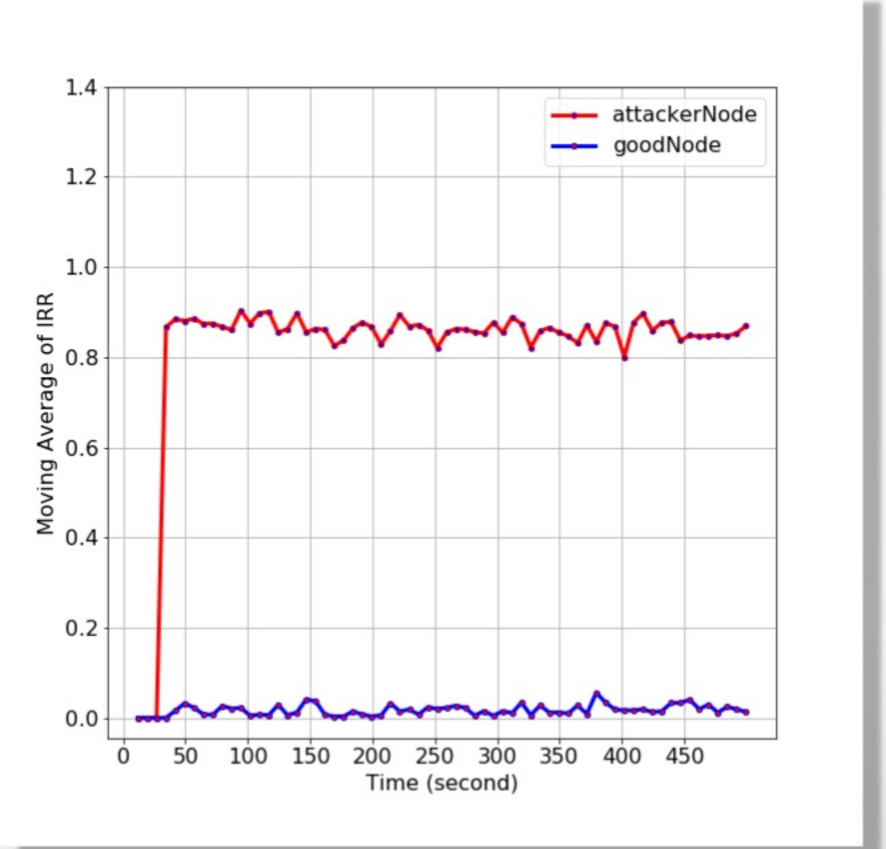


Figure 1: Scenario Malicious Node

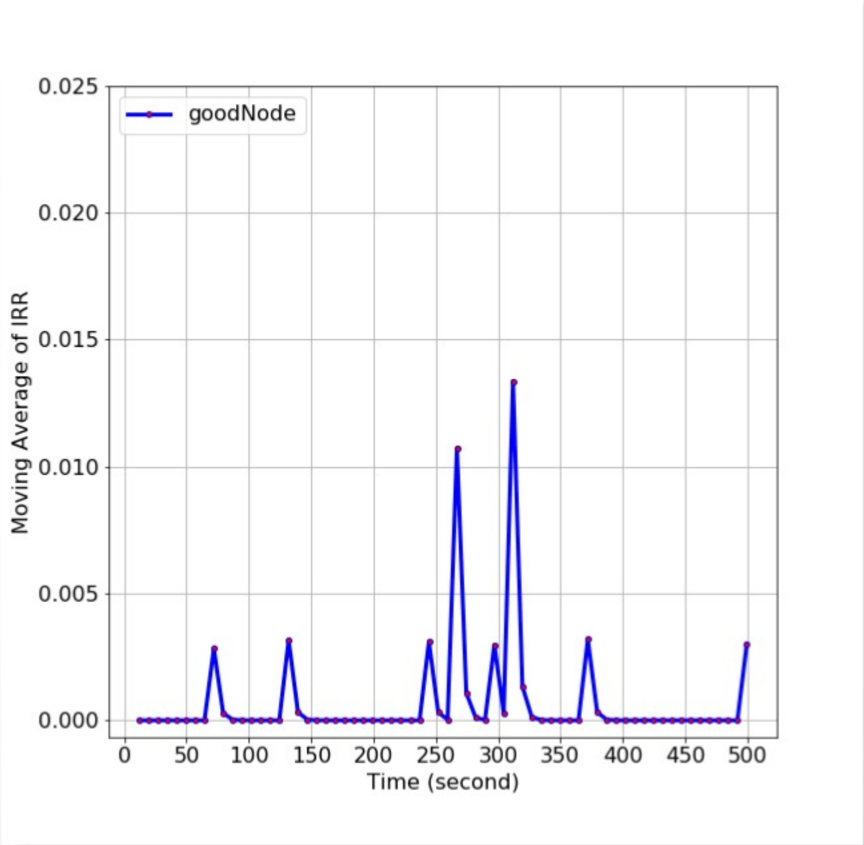


Figure 2: Scenario without Malicious Node

Observations

- High for Malicious Node
- Low for Well-behaved Node

Deviation of Moving Average of IRR..

- Calculated in Action phase after calculating moving Average of IRR.
- For each node we calculate the average of calculated moving Average of IRR of its neighboring nodes.
- Then calculate Deviation for each neighbor.

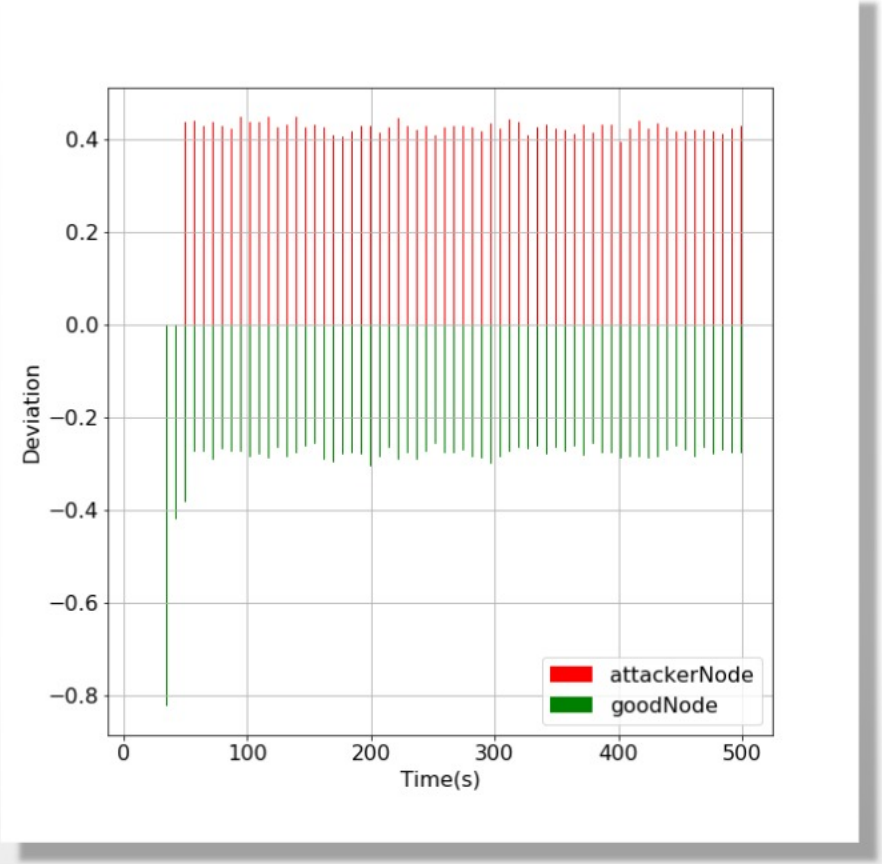


Figure 1: Scenario Malicious Node

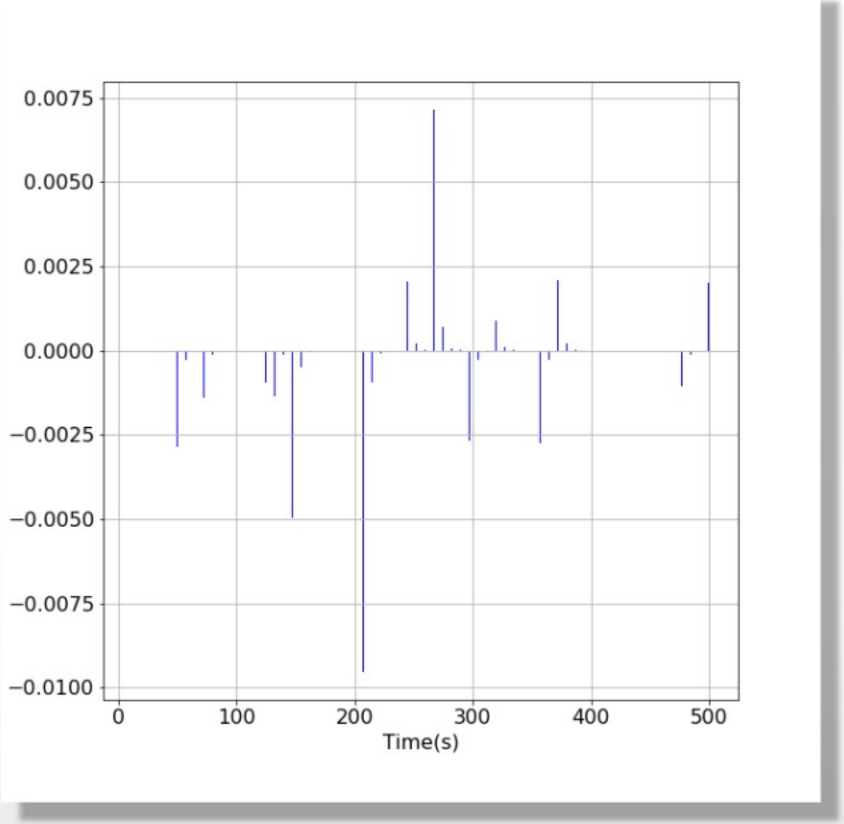


Figure 2: Scenario without Malicious Node

Observations

- Positive and High for Malicious Node.
- Negative or very low positive for Well-behaved node.

Moving Average of Inter Arrival time of RTS..

- Calculated continuously every time a new RTS packet is received from a specific neighbor.
- Calculate the Moving Average from data collected from Previous moving average and current Inter Arrival time of RTS.

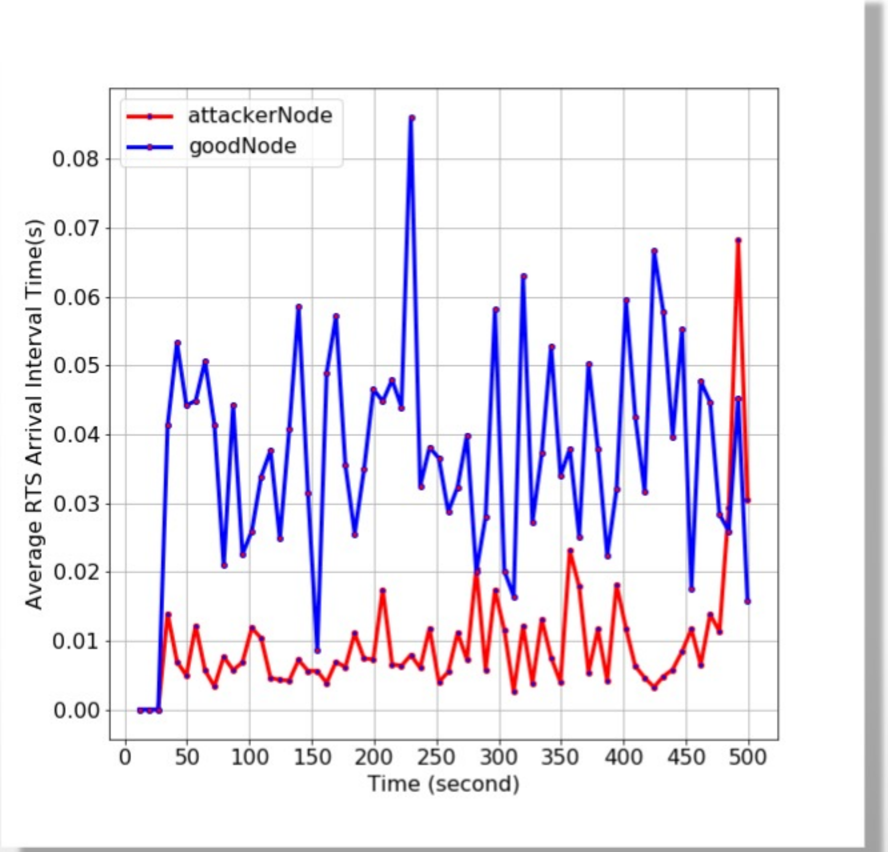


Figure 1: Scenario Malicious Node

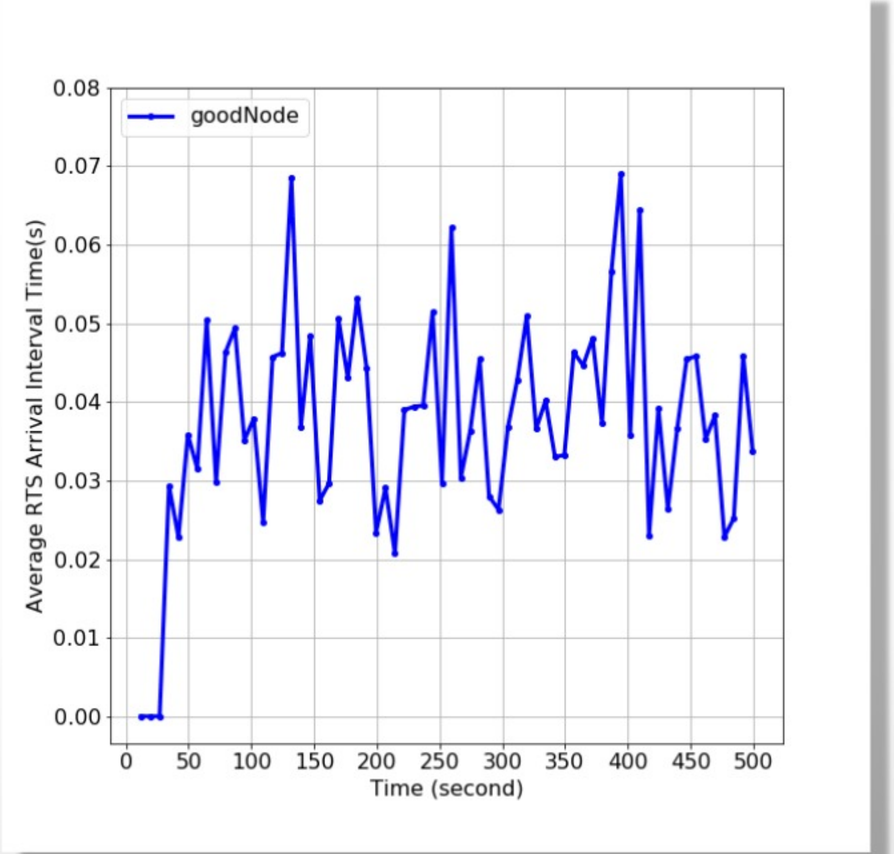
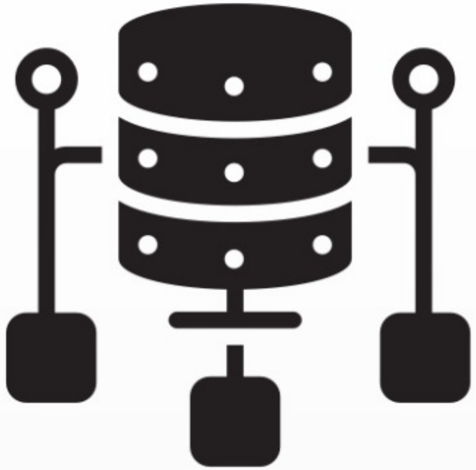


Figure 2: Scenario without Malicious Node

Observations

- Low for Malicious Node
- High for Well-behaved Node

Dataset..



No available dataset so far.

Generated random scenarios.

Collected samples from simulations run in Network Simulator 2.

Dataset description:

Number of Attributes	4
Number of Rows	2320449
Size	75 MB
Missing Data	No
Outliers	Present

Model Selection: Support Vector Machine..

- Linearly separable data.
- Linear Support Vector Machine approach can be used for learning.
- Train set= 80%
- Test set=20%
- SVM learns from the train set.
- Creates a hyperplane to classify well-bheaved and malicious nodes.

Trained Models Performance on Test Set..

False positive ratio and accuracy results.

Property	Value
False positive ratio	0.02788
Accuracy on Train Set	0.93005
Accuracy on Test Set	0.94070

Experimental Results..

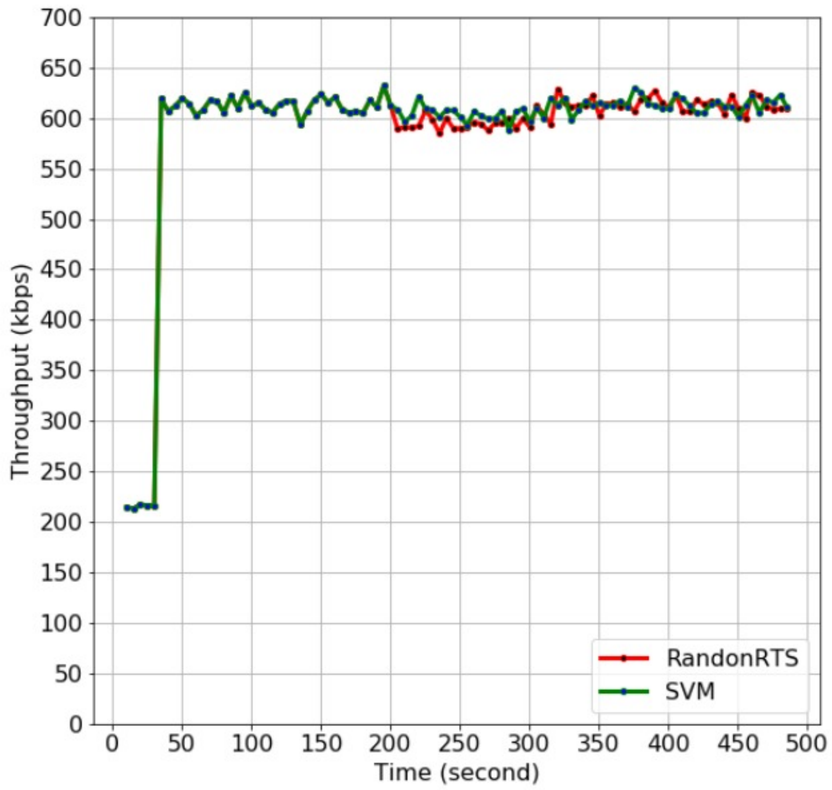


Figure A: Throughput comparison between Random RTS validation and SVM based classification

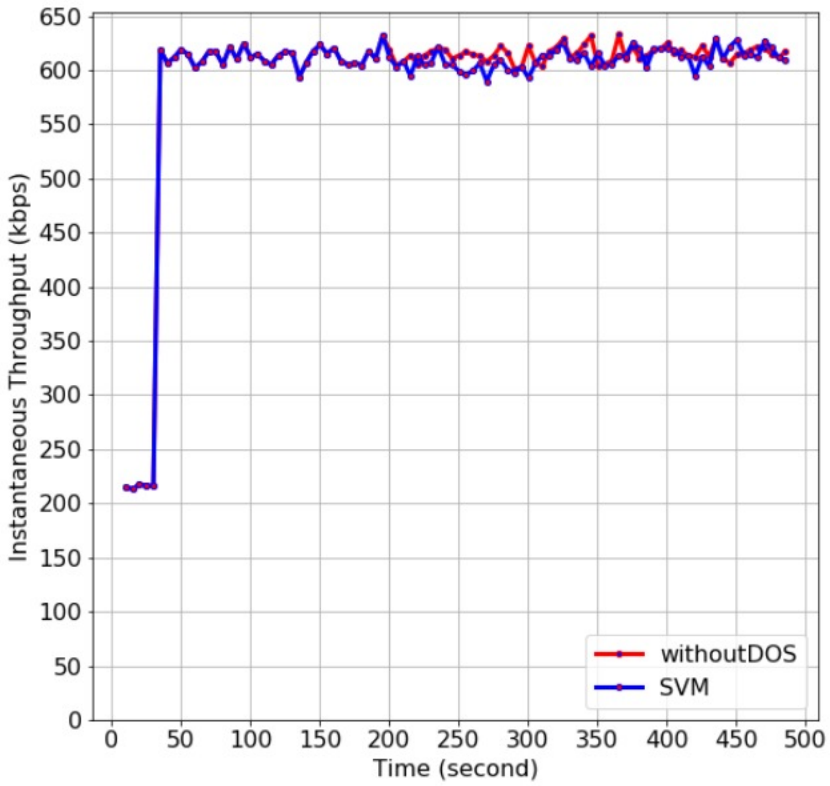


Figure B: Throughput comparison between without DoS and SVM based classification

Experimental Results..

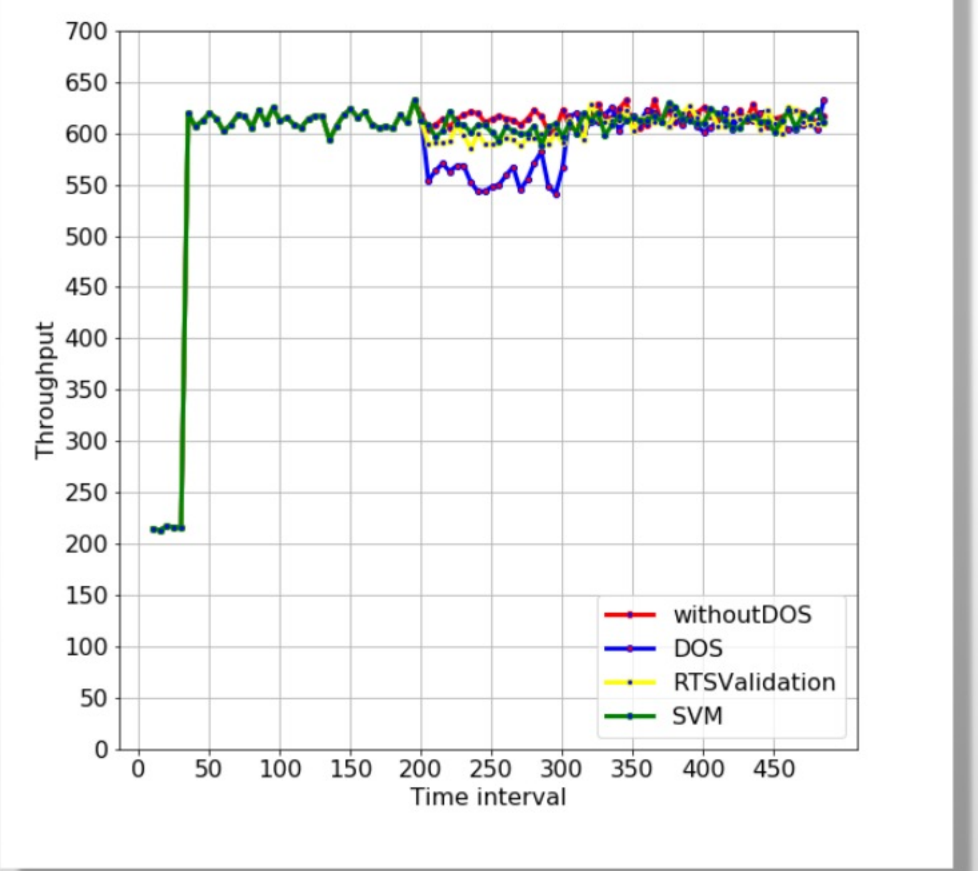


Figure C: Instantaneous throughput comparison under different approaches

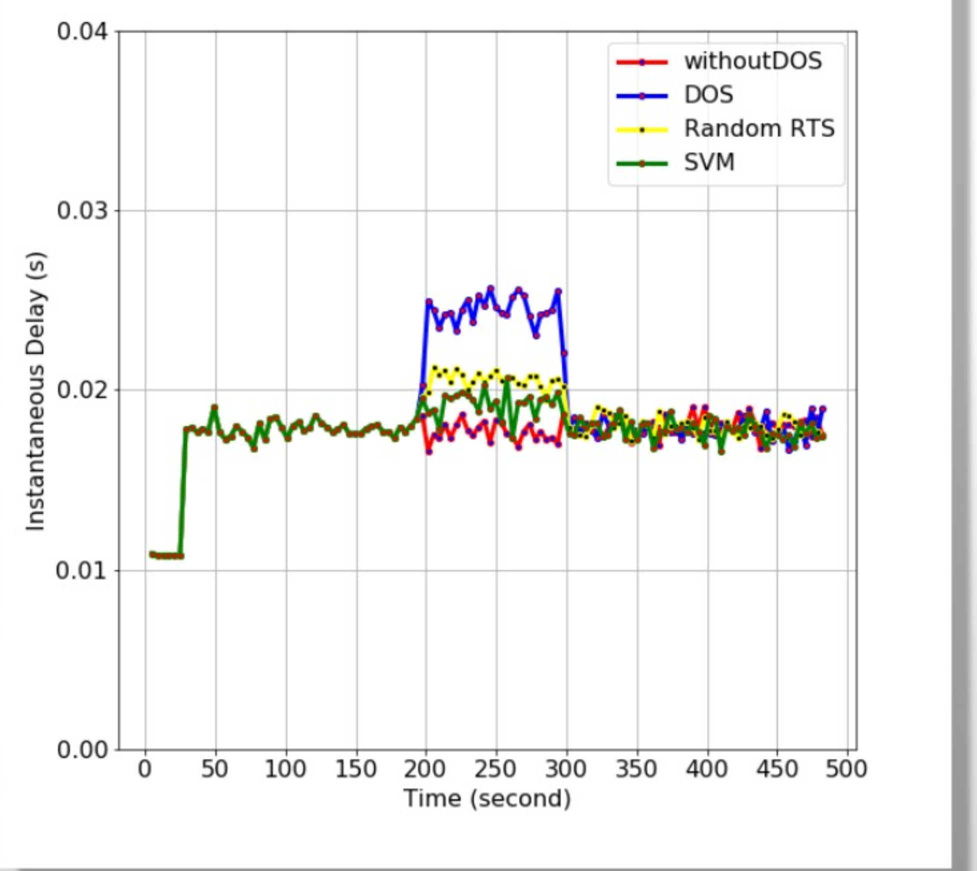


Figure D: Instantaneous Delay comparison under different approaches

Conclusion..

- Goal is to increase aggregate throughput more than Random RTS validation.
- Try to find a pattern to classify the good and the bad node.
- Introduce significant features so that machine can learn.
- After learning machine can take decision at the starting of action period.
- If machine take false decision, it will fix it in next action period after getting data from next learn period.

Future Works..

- We plan to carry out our work on different aspects.
- Tuning LAR ratio.
- Tuning features selection hyperparameters (coeffIRRL, coeffIRRA, coeffIAT)
- Classification based solution for CTS only attack.

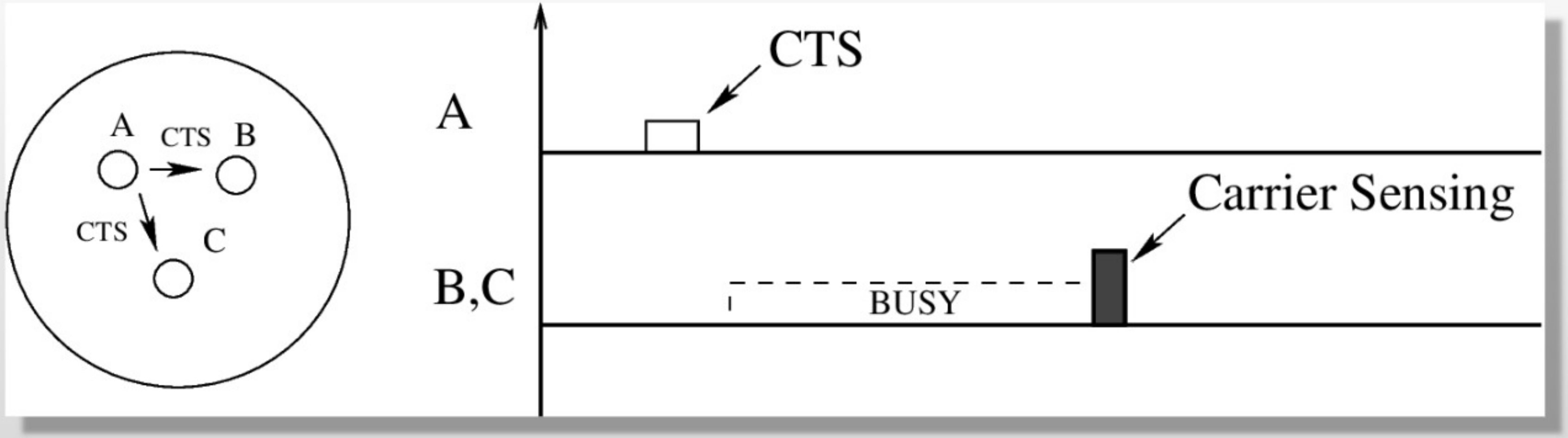


Figure: CTS only Attack

References

- [1] D. Chen, J. Deng, and P. K. Varshney. Protecting wireless networks against a denial of service attack based on virtual jamming. In The Ninth ACM Annual International Conference on Mobile Computing and Networking (MobiCom) Poster, September 2003.
- [2] Ashikur Rahman and Pawel Gburzynski. Hidden Problems with the Hidden Node Problem. In Proceedings of the USENIX Security Symposium, August 2003.

Thank You & Welcome! Questions?