Volume 4, Issue 4, April 2014 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

RTS/CTS Frame Synchronization to Minimize the Hidden Node Problem in Wireless Network

Supriya S. Sawwashere
Computer Science and Engineering
G. H. Raisoni College of Engineering
Nagpur (Maharashtra), India

Sonali U. Nimbhorkar
Department of Computer Science and Engineering
G. H. Raisoni College of Engineering
Nagpur (Maharashtra), India

Abstract— The use of wireless networks has been drastically increased due to the popularity of mobile devices, such as smart phones and tablet personal computers. In such scenario, a large number of devices associated with network can overlap with each other, causing the hidden-node problem to occur more easily. Hidden terminals are intermediate sources that can reduce the throughput of a wireless network if it applies MAC protocol. The RTS/CTS mechanism is a popular solution to this problem. RTS/CTS (Request to Send / Clear to Send) mechanism is a reservation scheme used in the wireless networks. It is used to minimize frame collisions created due to the hidden node problem. The attack made on this reservation scheme, called as RTS/CTS attack, comes under low rate DoS attacks. This paper mainly concentrates on the mechanism used to synchronize the packets sent by the sender nodes as well as by the receiver nodes.

Keywords— Denial-of-Service (DoS), RTS/CTS attacks, NAV, Node synchronizations, wireless network.

I. INTRODUCTION

The use of wireless network has been surprisingly increased since few years. The wireless networking protocol specifies a common MAC (media access control) layer. It provides variety of functions that support the operations of wireless LANs. In infrastructure mode of network, the centralized node is responsible for the channel allocation. In ad-hoc mode, the channel allocation is distributed. In wireless networking, the hidden terminal problem arises for a visible node from a wireless access point, rather than from other nodes communicating with the access point. This creates the problems in (MAC) media access control.

The hidden node problem can be explained by a simple example. Let the user A transmits the message to the user B, which is not known by the third user C. The user C also sends the message to B. The user B cannot recognize whether the message has been sent by either user A or B. this problem is termed as hidden node problem. This problem results in increasing the packet collisions, packet dropping problems as well as decreases the network performance, as the network gets busy for more than the desired time.

A simple and well-dressed solution to this hidden terminal problem is to use Request to Send/Clear to Send (RTS/CTS) frames. The RTS/CTS frames play the important role to avoid the hidden node problem created by mobile node in the ad hoc-based mobile LAN [12]. It is a handshaking mechanism to reserve the channel for a specific duration before actual data transfer starts. This mechanism generally works in the infrastructure mode. Figure 1 shows the use of RTS and CTS with the Network Allocation Vector (NAV) value set.

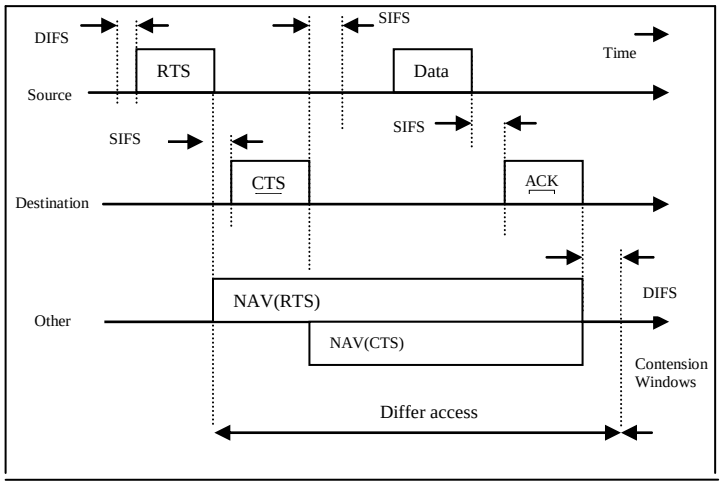


Figure1. RTS/CTS Communication with NAV

II. RTS/CTS MECHANISM

RTS/CTS mechanism is a three way handshaking system, consisting of RTS frame, CTS frame, ACKs. If a node needs to send a packet, it first requests for a channel by transmitting a RTS packet. Nodes that hear the RTS packet will defer transmission for a sufficiently long period of time to allow the transmitter to receive the CTS packet. If the channel is available, the receiver replies with a CTS packet. Nodes hear the CTS packet will back off for a period of time that is sufficiently long to allow the receiver to receive the entire data packet. After the sender receives the CTS packet successfully, it starts for the transmission of actual data packet.

A shown in the figure, after waiting for Distributed Inter Frame Space (DIFS) the sender sends a RTS packet with the receiver's address in the network. It includes the duration in terms of time limit required for the whole data transmission and the ACK related to it. Other nodes in the networks update their NAV value as:

NAV (RTS) =3*SIFS + Data +ACK

It specifies the maximum instance of time, when the other nodes can request for the resources again.

2	**2**	**6**	**6**	**6**	**Bytes**
Frame control	Duration	Receiver Address	Transmitter Address	FCS	

Figure2. RTS Frame

The receiver node receives the RTS frame and after SIFS (Short Inter frame Space), it replies with the CTS frame with the time duration field in the network to intimate the other nodes also. After receiving the packet from the receiver, the neighbor stations adjust their NAV. Other nodes in the networks update their NAV value as:

NAV (CTS) = RTS - (CTS + SIFS)

2	**2**	**6**	**4**	**Bytes**
Frame Control	Duration	Receiver Address	FCS	

Figure3. CTS Frame

The sender node cannot proceed for the transmission until it receives the CTS packet. Basically, this mechanism reserves the medium for one sender exclusively. Therefore it is called as virtual reservation scheme [18].

III. RELATED WORK

Wireless networks use the contention slots with the standard 802.11 protocol. The contention slots contain the RTS/CTS frame, which is a handshaking mechanism. These slots reserve the channel for a specific duration before starting the actual data transfer. The network is violated by DOS attacks, which is many times applied on the RTS/CTS frames. PMD Nagarjun et.al. [1] explained about the RTS/CTS attacks with its different scenarios in the wireless network. The attack exploits the medium reservation mechanism of 802.11 networks through duration field. Also they created an application to analyse the behaviour of attacks. Q. Gao, et. al. [3] studied the effects of power transmission and the contention slots (multiple RTS/CTS frames) used on a MIMO (Multiple Input Multiple Output) technique, which is a MAC protocol with multiple contention slots. They applied the joint optimization method on the transmission power of the nodes in the network and contention slots. This can improve the transport throughput of the network. Also they investigated that the increase in the bit rate can reduce the optimal number of contention slots. In [2] Minh1o Kim et. al., proposed a new HD mechanism, which is used to detect hidden terminals. The mechanism uses the statistics of measurable MAC layer with the received ACK frame. It also identifies whether there is a need of the RTS/CTS frame to exchange. Tao Xiong et.al.[4] proposed a symbol level detection mechanism, titled as RTS/S-CTS mechanism for silencing the hidden terminals. The mechanism reduces the packet collision occurred due to remote hidden terminals. They also proposed a self test/cancelation method to overcome the detection errors. Phil Karn [5] proposed a MACA system to make the channels busy using the RTS/CTS packets exchange without carrier sense. Lin Dai et. al. [6] presented the stability, throughput, and delay analysis of buffered IEEE 802.11 DCF networks. It has revealed that an IEEE 802.11 DCF network has two steady-state points. In [7], the effect of the 802.11-compliant RTS/CTS on TCP agents using plain and delayed ACKs has been compared. On the basis of comparison, they introduced Full, partial and No RTS/CTS functions to improve the spatial reuse in network. An analytical model was developed to calculate the average packet delay of 802.11 protocol, and the results shown that the RTS/CTS mechanism is most effective in the large network instead of small scenarios[8][9]. A feedback-based backoff-tuning strategy can be used to cover maximum throughput in the network [9]. RTS/CTS mechanism can reduce the number of retransmissions only if if the hidden node problem exists in various network scenarios [10]. Tian et. al. [11] analysed the interference avoidance scheme based on multi-frequency RTS/CTS CR scheme, in which the energy of CTS frame transfer is the main component to improve the performance of the scheme. John Bellardo et.al. [13], provided an analysis of attacks on 802.11 MAC protocol to mitigate the vulnerabilities, with their efficiency and potential low-overhead implementation changes. An NAV validation scheme can remove the

vulnerabilities and prevent the Denial of Service (DoS) attack based on virtual jamming [14]. The jamming signal on DSSS physical layer stops the 802.11b mode and 802.11b/g multi-mode networks and also the MAC attacks stop the working of network [15]. Also they suggested the modulation change techniques to prevent these attacks. The misbehaviour of greedy receiver may reduce the performance of the network tremendously, that may create the starvation problem also [16]. Rate adaption method can solve this problem in order to prevent these mishaps like faking ACKs, spoofing ACKs, etc. The vulnerabilities like the false CTS and false packet validation attacks which exploit the CTS and ACK packet formats are analysed at the MAC layer [17]. These types of attacks can harm the prestige of the loyal node; even it can destroy the node's belief. Xiaocheng Zou et.al. [18] investigated the fabricated CTS attacks in MAC protocol, in which false CTS packets with large NAV values is sent by the attacker node to reserve the shared channel. AIS (Address Inspection Scheme) can destroy such jamming attacks. Nodes can differentiate the legal CTS packets from fabricated ones by observing the destination address with the help of tow-hop neighborhood information. K. Sugantha et al. [19] proposed the statistical method to detect the misbehaviour due to NAV attack. It has been proved that that most of the communications are suspected from the virtual carrier sense mechanism, to prevent the collisions from hidden nodes. Changwang Zhang et. al [20] proposed an efficient method to detect and remove TCP-targeted LDDoS attacks based on a novel metric – Congestion Participation Rate (CPR). Hsueh-Wen Tseng et.al. [21] proposed the scheme that detects the hidden devices addresses based on the overlapped signals in the physical layer, and the doubtful addresses are checked by the HDP address verification procedure performed in the MAC layer. Minho Kim et. al. [22] proposed a novel HD mechanism, which implemented by using some new features in IEEE 802.11n system. it detects hidden nodes in which frames can be lost due to any combination of collisions, hidden nodes, and channel impairments. Kyung Jae Kim et. al. [23] proposed OSA protocols in the single channel and the multi-channel cognitive radio networks with one control channel and several licensed channels where a slot is divided into contention phase and transmission phase.

IV. PROPOSED METHODOLOGY

The attacker nodes in the wireless network keep the channel busy for an additional time by changing the duration field value of the RTS packets. Since legitimate nodes will obviously respond to RTS request with CTS frame, an attacker could exploit legitimate nodes to disseminate CTS with manipulated duration field, which causes the attack automatically. These types of attacks on RTS /CTS frame can be identified and removed in order to improve performance efficiency, throughput of network. The packet synchronization mechanism can be applied to do so. The algorithm is as follows:

1. Deploy the nodes.
2. Use RTS & CTS frames for reliable communication.
3. Set the maximum number of packets to be sent by the requesting node/replying node as a Packet_Threshold.
4. Check for each requesting/replying node

```
{
  If Packet_Sent > Packet_Threshold then
    Declare the node as the attacker node.
    Block that node.
}
```

5. Display the list of blocked nodes in the network.

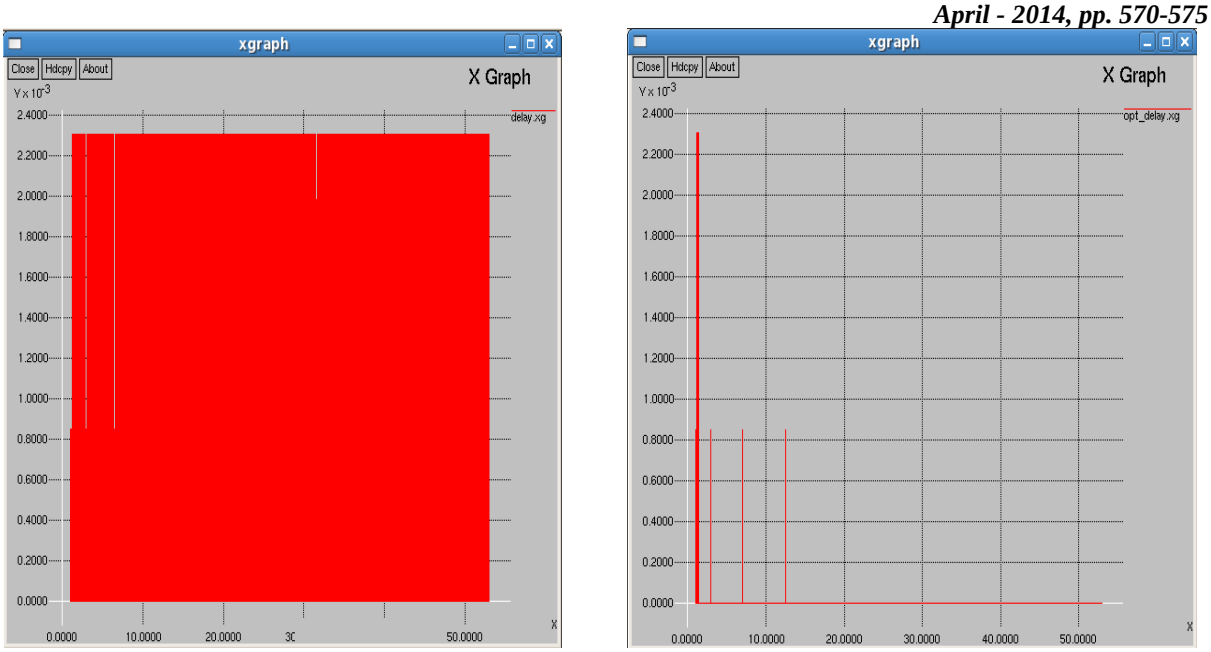
The blocked node will not be able to participate in the further transmissions.

V. SIMULATION AND RESULTS

Network Simulator 2.35 has been used for the simulation. Total number of 50 nodes are used for the simulation. The interface queue type is set as Droptail. The network performance parameters are compared by using graphs such as transmission delay, jitter, throughput, energy remained after packets transmission. Table 1 shows all the necessary parameters which are set at the time of execution. The graphs for both the conditions are compared. Part (a) in each of the figures illustrates the parameters for the transmission without using the Packet synchronization and part (b) with using the packet synchronization algorithm. The packet synchronization algorithm blocks the detected nodes, which are the parts of the network.

Table I. Simulation parameters

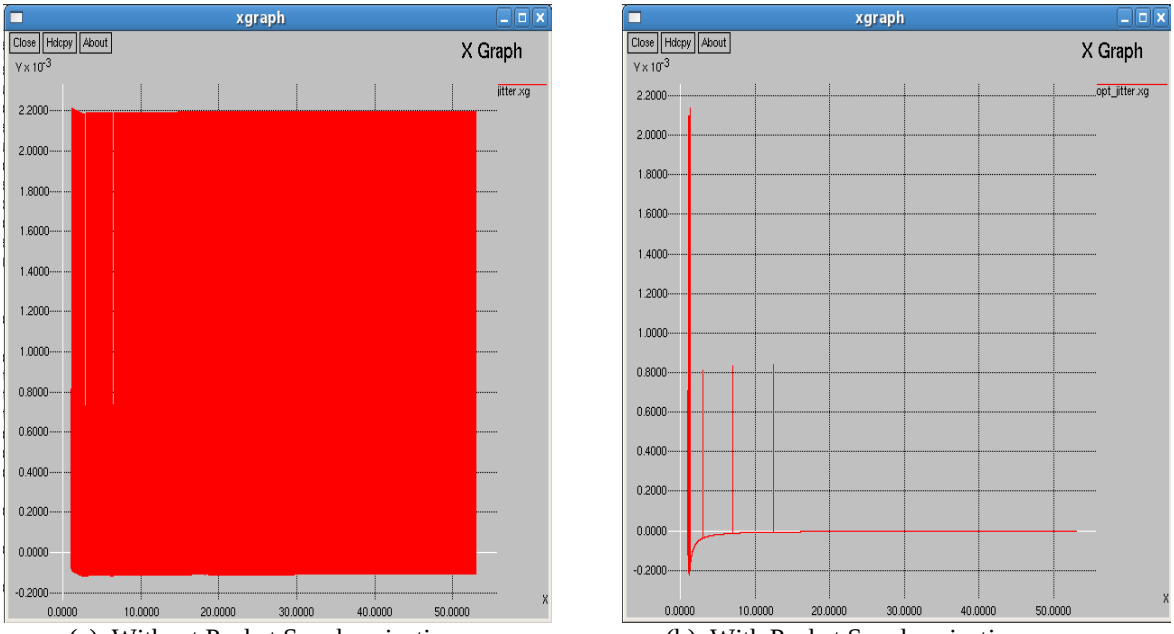
Parameter	Value
Simulator	NS2.34
Simulator Time (s)	50 seconds
Number of Nodes	50
Simulation Area	300*300
Routing Protocol	AODV
Traffic	CBR (UDP)
MAC Layer Protocol	IEEE802.11



(a) Without Packet Synchronization (b) With Packet Synchronization

Figure4. Comparision of Transmission Delay

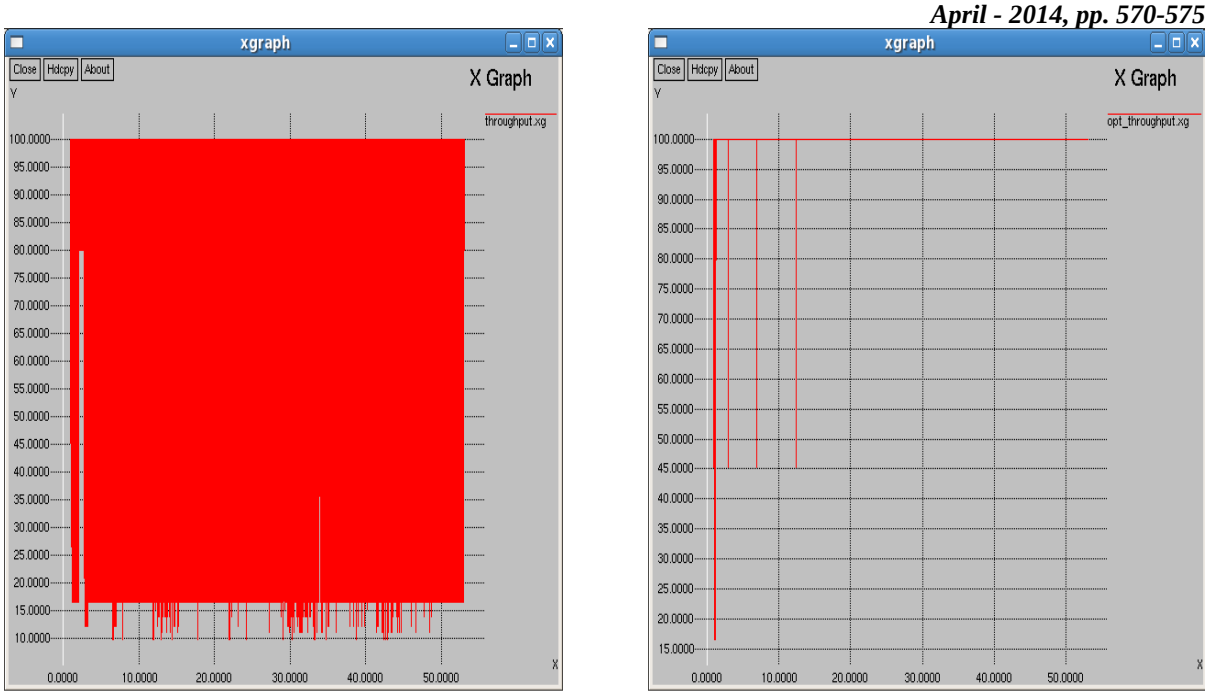
- Delay: Delay is an important characteristic for measuring the network performance. It can be defined as the difference between the time at which the node transmits the packet and the time at which the packet is received by the other node. It is measured in seconds. As shown in figure 4, the transmission delay can is minimized by using packet synchronization algorithm as compared with other one figure (a).



(a) Without Packet Synchronization (b) With Packet Synchronization

Figure 5. Comparision of Jitter

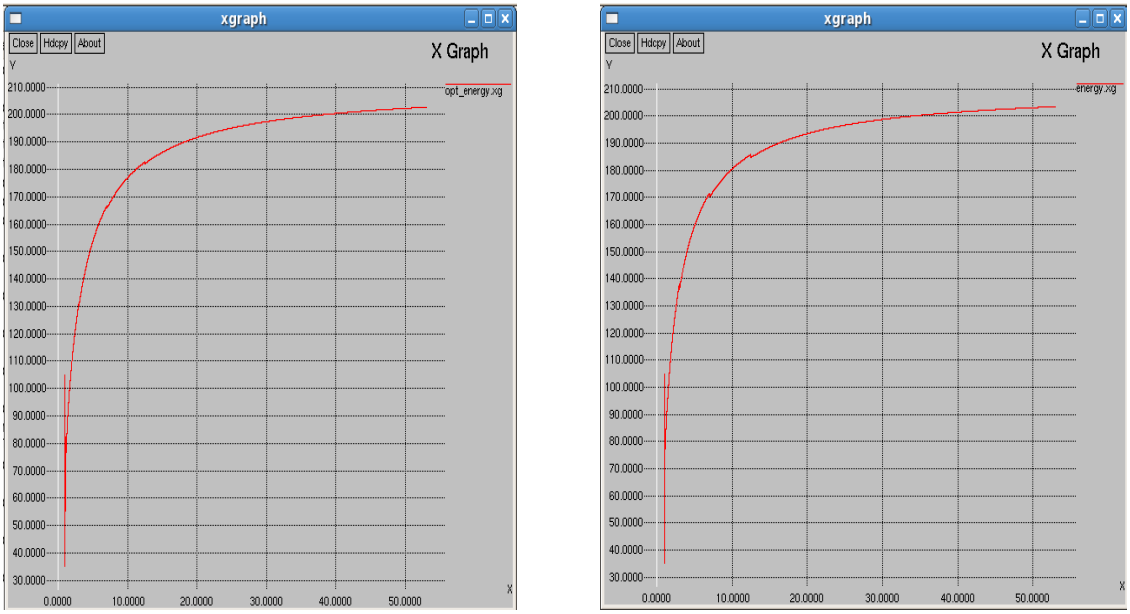
- Network Jitter: Jitter of the network is calculated as the difference between the total delay and the mean delay, which is the delay per count. The jitter is calculated without applying the algorithm and also by using the algorithm. The results are shown in figure 5. By applying the algorithm, the jitter is reduced at much extent.



(a) Without Packet Synchronization (b) With Packet Synchronization

Figure 6. Comparision of Performance Throughput

- Throughput: The complete performance of the network in terms of successful transmission out of the desired complete transmission. The use of algorithm has improved the throughput of the network much more than the other one. The improvement is illustrated in figure 6.



(a) Without Packet Synchronization (b) With Packet Synchronization

Figure 7. Comparision of Energy Consumption

- Energy: The power can be measured in terms of energy consumption in the network for the complete communication. The increase in number of request/reply frame transmissions requires more energy consumption. The limitation applied on the count of the packets reduces the energy consumption of the network. In figure 7 the green coloured graph show that the energy consumption is reduced as compared to the red coloured graph.

VI. CONCLUSION

We have proposed the packet synchronization mechanism that is simple to implement and minimizes the attacks made on the RTS/CTS frames. The attacker nodes are identified and removed for the further participation in the communication. It also minimizes the number of faulty packets and dropping of them.

The results are compared between the transmission without mechanism and with mechanism. The use of mechanism decreases the communication delay, jitter, energy consumption resulting to the increase in the performance throughput.

REFERENCES

[1] PMD Nagarjun, V. Anil Kumar, Ch Aswani Kumar, Ahkshaey Ravi "*Simulation and Analysis of RTS/CTS DoS Attack Variants in 802.11 Networks*", IEEE Proceedings of the 2013 International Conference on Pattern Recognition, Informatics and Mobile Engineering (PRIME) February 21-22.

[2] Minho Kim,Student Member, IEEE, and Chong-Ho Choi, "*Hidden-Node Detection in IEEE 802.11n Wireless LANs*", IEEE Transactions On Vehicular Technology, Vol. 62, No. 6, July2013.

[3] Q. Gao,L. Fei, J. Zhang, X.-H. Peng, "*Performance optimisation of a medium access control protocol with multiple contention slots in multiple-input multiple-output ad hoc networks*", IET Commun., 2010, Vol. 4, Iss. 5, pp. 562–572.

[4] Tao Xiong, Jin Zhang, Junmei Yao and Wei Lou, "*Symbol-Level Detection: A New Approach to Silencing Hidden Terminals*", Hong Kong RGC (PolyU521312), Hong Kong PolyU (A-PL84, A-PJ16), and National Natural Science Foundation of China (No. 61272463).

[5] P. Karn, "*MACA- A New Channel Access Method for packet Radio*," in the 9th ARRL Computer Networking, 1990.

[6] Lin Dai and Xinghua Sun "*A Unified Analysis Of IEEE 802.11 DCF Networks: Stability, Throughput, And Delay*", IEEE Transactions On Mobile Computing, Vol. 12, No. 8, August 2013.

[7] Stylianos Papanastasiou, Mohamed Ould-Khaoua, Vassilis Charissis, "*The effect of the RTS/CTS handshake on TCP",* 21st International Conference on Advanced Information Networking and Applications Workshops, 2007, AINAW '07, pp. 940 – 946.

[8] P. Chatzimisios, A.C. Boucouvalas and V. Vitsas, "*Packet delay analysis of IEEE 802.11 MAC protocol*", Electronics Letters 4th September 2003 Vol. 39 No. 18.

[9] Rsffaele Bruno, Marcn Conti, Enncn Gregnri, "*IEEE 802.11 Optimal Performances: RTS/CTS Mechanism Vs. Basic Access*", NATO Science Program in the Collaborative Linkage Graot PST.CLG.977405, 2002.

[10] Hetal Jasani, Nasser Alaraje, "*Evaluating the Performance of IEEE 802.11 Network using RTS/CTS Mechanism*", IEEE EIT 2007 Proceedings.

[11] Tian TIAN, Hisato IWAI, Hideichi SASAOKA "*Statistical Analysis of Interference Avoidance based on Multi-Frequency RTS/CTS Cognitive Radio*" 2011 6th International ICST Conference on Cognitive Radio Oriented Wireless Networks and Communications (CROWNCOM).

[12] Ha Cheol Lee "*The Effect of RTS/CTS Frames on the Performance of Ad Hoc-Based Mobile LAN*" 2010, 3rd International Conference on Advances in Mesh Networks, IEEE.

[13] J. Bellardo and S. Savage, "*802.11 Denial-of-Service attacks: Real vulnerabilities and practical solutions*," 12th USENIX Security Symposium, Washington D.C., USA, vol. 12, pp. 2-2, Aug. 2003.

[14] Dazhi Chen, Jing Deng and K. Varshney Pramod, "*Protecting wireless networks against a Denial of Service attack based on Virtual jamming*," MobiCom 2003, CA, USA, Sept. 2003, unpublished.

[15] Bo Chen, Muthukkumarasamy and Vallipuram, "*Denial of Service attacks against 802.11 DCF*," IADIS International Conference: Applied Computing, pp. 552-556, 2006.

[16] Mi Kyung Han and Lili Qiu, "*Greedy receivers in IEEE 802.11 Hotspots: impacts and Detection*," Dependable and Secure Computing,vol. 7, pp. 410-423, 2010.

[17] Abderrezak Rachedi and Abderrahim Benslimane, "*Smart Attacks based on Control Packets Vulnerabilities with IEEE 802.11 MAC*," The International Wireless Communications and Mobile Computing Conference (IWCMC'2008),Crete Island : Greece (2008).

[18] Xiaocheng Zou and Jing Deng, "*Detection of Fabricated CTS Packet Attacks in Wireless LANs*", Institute for Computer Sciences, Social Informatics and Telecommunications Engineering LNICST, pp. 75–85, 2011.

[19] K. Sugantha and S. Shanmugavel, "*A statistical approach to detect NAV attack at MAC layer*," International Workshop on Wireless Ad-hoc Networks, London, UK, 2005

[20] Changwang Zhang, Zhiping Cai, Weifeng Chen, Xiapu Luo and Jianping Yin, "*Flow level detection and filtering of low-rate DDoS*", Computer Networks 56 (2012) 3417–3431.

[21] Hsueh-Wen Tseng, Shan-Chi Yang, Ping-Cheng Yeh, and Ai-Chun Pang "*A Cross-Layer Scheme for Solving Hidden Device Problem in IEEE 802.15.4 Wireless Sensor Networks*", IEEE Sensors Journal, Vol. 11, No. 2, February 2011.

[22] Minho Kim and Chong-Ho Choi, "*Hidden-Node Detection in IEEE 802.11n Wireless LANs*", IEEE Transactions On Vehicular Technology, Vol. 62, No. 6, July 2013.

[23] Kyung Jae Kim, Kyung Sup Kwak, and Bong Dae Choi, "*Performance Analysis of Opportunistic Spectrum Access Protocol for Multi-Channel Cognitive Radio Networks*" Journal Of Communications And Networks, Vol. 15, No. 1, February 2013.

