Journal of Computer Science 5 (3): 214-220, 2009
ISSN 1549-3636

Empirical Analysis of Virtual Carrier Sense Flooding Attacks Over Wireless Local Area Network

Mina Malekzadeh, Abdul Azim Abdul Ghani, Jalil Desa and Shamala Subramaniam
Faculty of Computer Science and Information Technology,
University of Putra Malaysia, Malaysia

Abstract: Problem statement: Wireless Local Areas (WLANs) are subject to different types of vulnerabilities. Denial of Service (DoS) attack is the most current challenging issue on the WLANs. The objectives of the study were to (i) Provide an empirical analysis to conduct a series of wireless virtual carrier sense DoS attacks using wireless control frames vulnerabilities, (ii) Design a testbed to compared and analyzed the damage that these attacks can imposed on wireless networks, and (iii) Evaluated the effectiveness of such attacks on performance of WLAN in term of data transmission rate. **Approach:** The testbed employed ubuntu distribution along a network analyzer, Atheros chipset, and frame injection to the tested WLAN. All experiments were placed on two phases: Targeting wireless access point and targeting wireless client. Each phase presented the results of experiments under three circumstances: Before, during, and after the attacks. **Results:** Even when virtual carrier sense communication was disabled in the tested WLAN, still the target nodes answered to these forgery frames which made the attacks easier. Attacks over the wireless clients were more effective than the access point. In VCS-RTS-C the rate of data transmission from 3547.384 B $\sec^{-1}$ decreased to 9.185 B $\sec^{-1}$. In contrast with VCS-CTS-C, it decreased from 4959.887-44.740 B $\sec^{-1}$ and amount of decrease for VCS-ACK-C was from 7057.401-136.96 B $\sec^{-1}$. The obtained results demonstrated that during the attacks the target clients were completely disconnected from the wireless network and unable to do any communication. **Conclusion:** The influence of wireless virtual carrier sense attacks on performance of the wireless network was analyzed. The data transmission rate of the tested WLAN under the attacks was compared with the transmission rate of the WLAN operated under normal conditions. The obtained results confirmed the attacks could easily overwhelmed and shut down the wireless network.

Key words: DCF flooding, control frame attack, virtual carrier sense attack, wireless network DoS attacks, NAV attack, RTS/CTS/ACK attack

INTRODUCTION

Security is the most important issue in any communication network. IEEE 802.11 has ratified a variety of security protocols to provide a secure wireless communication. Protocols such as WEP, WPA and the 802.11i have been ratified to provide data frames security. IEEE 802.11i uses a strong algorithm like AES to make a secure channel. But all these security protocols merely provide data frame protection and other wireless frames such as control frames are transmitted clearly without any protection[1]. An attacker can take this advantage to start Virtual Carrier Sense Flooding (VCSF) attacks by using unprotected control frames over the wireless networks.

The focus of this research is to investigate practical attacks over the wireless networks using control frames vulnerabilities in virtual carrier sense. We design a wireless LAN environment testbed to identify the impact of these attacks on transmission rate of the wireless network.

IEEE 802.11 media access control: 802.11 wireless networks use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) to avoid simultaneous access (collisions) by deferring access to the medium. Carrier sensing is used to determine if the medium is available. Two types of carrier sensing functions in 802.11 manage this process: The physical carrier sensing (which is done through hardware by CCA) and virtual carrier sensing (which employs control frames transmission)[2,3].

Control frames: In wireless networks control frames assist in the delivery of data frames. They administer

Corresponding Author: Mina Malekzadeh, Faculty of Computer Science and Information Technology, University of Putra Malaysia, Malaysia

access to the wireless medium and provide MAC layer reliability functions. There are different types of control frames[2,3]. The most important of them are Request-To-Send (RTS), Clear-To-Send (CTS) and Acknowledgment (ACK) frames which are shown in Fig. 1-3 respectively.

Virtual carrier sense: Virtual carrier sensing is provided by the Network Allocation Vector (NAV). NAV is a counter that lets the station to transmit its data if its value is equal zero. If carrier sensing function indicates that the medium is busy, all stations set their NAV and must wait to observe an idle media[2,3]. When media is free, stations can access the media to transmit their information. The standard defines two medium access methods: Point Coordination Function (PCF) and Distributed Coordination Function (DCF). DCF is mandatory and most wireless traffics use the DCF to access the media. If a station has a packet to transmit, it checks if the medium is idle for a Distributed Inter-Frame Space (DIFS) time. If the channel is idle, it sends the packet. If the channel is busy at any time during sensing, the node waits until transmission stops then waits for a further DIFS and contention period. If the channel is still idle at the end of the contention period the node transmits its packet otherwise it repeats contention process until it senses a free channel. After transmission of the data, the recipient sends an ACK control frame to inform a successful reception.

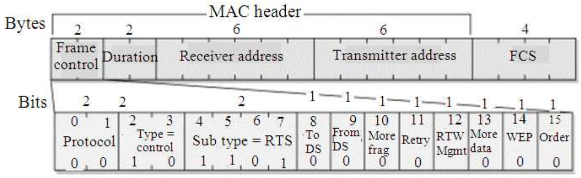

Fig. 1: RTS control frame structure

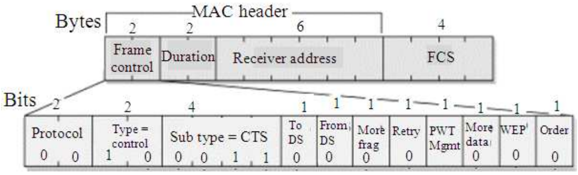

Fig. 2: CTS control frame structure

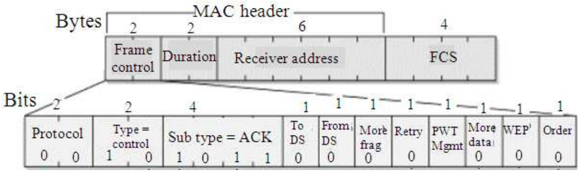

Fig. 3: ACK control frame structure

Sometimes wireless nodes can not hear each other which identify hidden nodes. Since the nodes can not hear each other they may sense media free at the same time and both tries to transmit simultaneously which makes collision on the network. Therefore to avoid hidden nodes problem the 802.11 standard defines an optional feature which includes the RTS/CTS function to control station access to the medium. If a station has a packet to transmit, it sends a RTS frame to the destination station. The destination station acknowledges the frame by sending CTS back to the sender. All stations that hear these RTS or CTS must defer to transmit according to the time specified in the duration fields of these frames. The sender transmits data and if the destination receives the packet without errors, it sends an ACK frame back to the sender[2,3]. Otherwise, the sender assumes that the packet has not arrived and it retransmits it again. If the medium is busy, the station defers until the medium is idle for a DIFS time and the contention process like before.

VCSF attack: RTS, CTS and ACK, each has a duration field in microsecond which indicates the amount of time that packet sender keeps the media busy to avoid other wireless nodes to transmit simultaneously. This field is 16 bits with a fix zero last bit therefore it has 2^{15} possible values with a maximum value about 32767 microseconds.

Since RTS, CTS and ACK frames are transmitted clearly, any attacker can exploit this feature to make a forgery frame and continually transmits that to the victim with maximum value for its duration filed. All nodes must set their NAV to this maximum value which keeps them silent and they have to wait until NAV becomes zero. If attacker continually sends his forgery control frames with maximum NAV value, he can prevent other nodes to access to the media and avoid them from transmission which can bring the network down and stop legal transmissions[8,9]. Sending RTS is more effective than the other attacks. Since according to the IEEE 802.11 standard, when a station receives a RTS control frame, it has to answer by sending CTS control frame. This can propagate the attack and give the attacker more chance to have a successful attack[10-12].

Related works: There are a few researches that have been done to implement VCSF over the wireless networks to test their effects on the WLAN performance in term of availability. For example, Bellardo *et al.*[4] have investigated the availability attacks over the wireless networks by using both management frames and control frames. They also demonstrated the DoS attack against the 802.11 DCF through a simulation study.

Chen *et al*.[5] considered the DoS attack against the 802.11 DCF in MAC layer by virtual jamming through injecting control frames. They also suggested a possible countermeasure in the form of NAV validation. They mentioned that the station which received RTS or CTS must wait the required time to observe the data transmission but if it could not observe any traffic the station can resets its NAV to zero which allows it to transmit its own traffic.

Chen *et al*.[6] investigate both Physical layer and MAC layer attack in wireless network. They identified that jamming signal generated by the 802.11b network card will stop the networks. They also demonstrated that the MAC attacks also can stop network functions. They conclude that any current or upcoming 802.11 standards would not provide any help to mitigate the risk of DoS attacks against the 802.11 DCF. Sugantha and Shanmugavel[7] investigated the vulnerabilities of the NAV and corresponding attacks. Their results show that the NAV attack can under perform the standard 802.11 MAC protocol. In[8] Pelechrinis considered possible signal jamming in the 802.11 standard and concluded that there is no solution that can fully address the problem of jamming in wireless networks.

However, no work has been done on investigating the effect of DCF vulnerabilities in case of virtual carrier sense attacks on performance of the 802.11 wireless networks in term of transmission rate, which has been presented in this study.

MATERIALS AND METHODS

Testbed environment: We implemented present experiment in presence of the current security protocols IEEE 802.11i. A testbed experimental environment is shown in Fig. 4.

From the Fig. 4, the tested WLAN includes a linksys wireless router WRT54G as a base station. Three legal wireless clients are equipped with IEEE 802.11g Intel chipset wireless adapter and they are running on Windows XP with service pack2. Another wireless client is used as a network analyzer to capture all frames transferred over the tested WLAN. A traffic analyzer is installed on this client to analyze the captured frames in monitor mode. It uses wireshark application to trace attacker path and keeps tracks of all the attacks which are used to present the results of the experiments. Both network analyzer client and attacker client are equipped with IEEE 802.1g Atheros chipset AR5212 wireless adapter and they are running on Ubuntu Gusty 7.10. The attacker client is using file2air application as frame injection tool. All the clients and wireless router support 802.1x user authentication.

To conduct our research, we differentiate between the attacks that target the wireless access point and the attacks that target a specific wireless client. The experiments consist of two phases as follow:

Phase 1: Virtual carrier sense attacks over the target access point. In this case three types of attacks are implemented as follow:

- VCSF attack by using RTS on access point (VCSF-RTS-AP)
- VCSF attack by using CTS on access point (VCSF-CTS-AP)
- VCSF attack by using ACK on access point (VCSF-ACK-AP)

The process of these attacks is shown in Fig. 5.

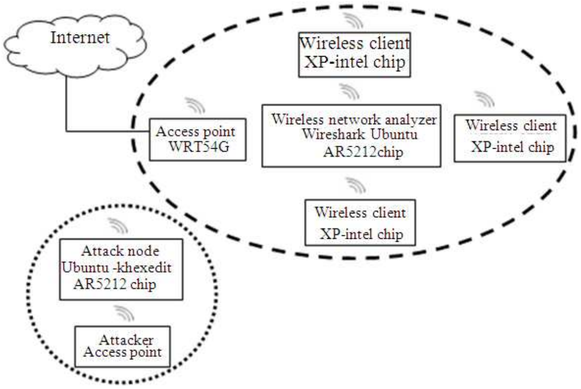
Internet
Wireless client XP-intel chip
Access point WRT54G
Wireless network analyzer Wireshark Ubuntu AR5212chip
Wireless client XP-intel chip
Wireless client XP-intel chip
Attack node Ubuntu -khexedit AR5212 chip
Attacker Access point

Fig. 4: Testbed Environment for VCSF Attacks over WLAN

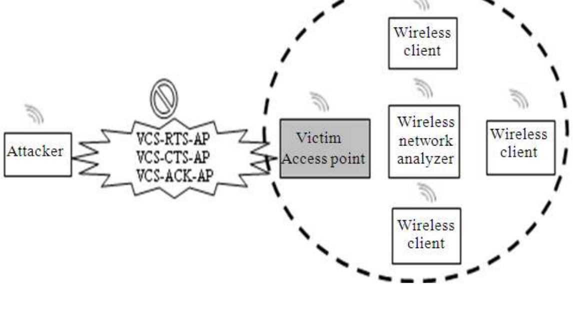

Fig. 5: Experimental Setup for VCSF Attacks over the Access point

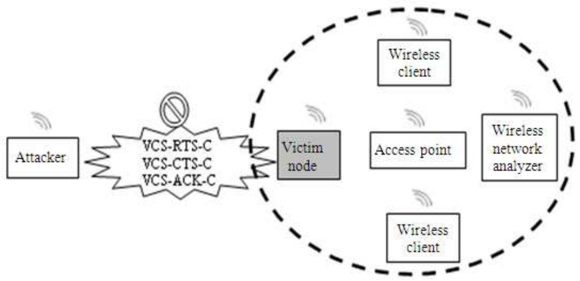

Fig. 6: Experimental setup for VCSF attacks over the client

Phase 2: Virtual carrier sense attacks over the target client. In this case three types of attacks are implemented as follow:

- VCSF attack by using RTS on a specific client (VCSF-RTS-C)
- VCSF attack by using CTS on a specific client (VCSF-CTS-C)
- VCSF attack by using ACK on a specific client (VCSF-ACK-C)

The process of the attacks shown in Fig. 6.

To implement the attacks as shown in Fig. 5 and 6, we used a customizable hex editor in Ubuntu Linux which is called khexedit. Through the editor, the forgery ACK, RTS and CTS frames were injected to the victim access point or client node. By implementing these experiments, we quantify the transmission rate of the tested WLAN to evaluate the impact of these attacks on the wireless network performance.

RESULTS AND DISCUSSION

Experiments analysis and measurement results: We ran experiments to evaluate and compare the performance of the wireless networks under the mentioned attacks. We illustrate how the attacks can degrade the transmission rate of the wireless network. In all the following experiments, the transmission rate is considered as our performance measure which is total bytes received at receiver side per second under different circumstances. Also to make our attacks more efficient, we set maximum duration value i.e., 32767 micro sec, in all our forgery frames when we are making them.

Experiment 1: Transmission rate measuring for VCSF-ACK-AP: For this experiment, we set more fragment bits in the forgery ACK frame to pretend the sender has more data to transmit which reserves channel longer and makes the attack more competent.

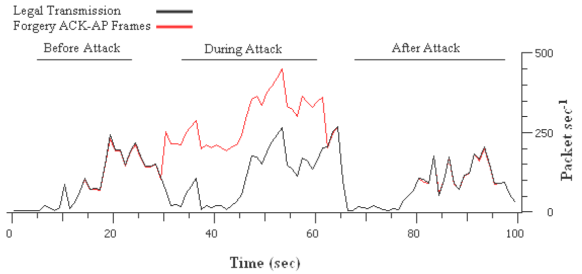

Fig. 7: Virtual carrier sense attack over access point using ACK flooding

After making our forgery ACK frame, we injected that continually to the victim access point to observe the results of the attack. Concurrently we kept the track of these forgery frames by our analyzer client to investigate any difference in transmission rate of the victim in the tested wireless network. The results are shown in Fig. 7 in three states: before, during and after VCS-ACK-AP attack over the tested WLAN.

As we can see from the Fig. 7, the attack duration is 33 sec which started from 29 sec till 62 sec. We measured the average of number of bytes per seconds for data transmission before and during the attacks to evaluate the effect of the attack. The results are as follow:

- Average transmission rate of WLAN before VCS-ACK-AP = 6144.331 B sec^{-1}
- Average transmission rate of WLAN during VCS-ACK-AP = 5914.193 B sec^{-1}

As the results show, this attack has a less effect on the performance of the wireless network. The attack affected the network communication and made it slower however all the nodes could communicate with each other during the attack.

Experiment 2: Transmission rate measuring for VCSF-ACK-C: We repeated the last experiment over a specific client in the tested WLAN. The result of the transmission rate of the network for the victim under the attack is shown as Fig. 8 in three states: before, during and after VCS-ACK-C attack over the tested WLAN.

From Fig. 8, the attack duration is 33 sec which started from 28 sec till 61 sec. During this time the average of transmission rate has been measured as follow:

- Average transmission rate of the victim before VCSF-ACK-C =7057.401 B sec^{-1}
- Average transmission rate of the victim during VCSF-ACK-C =136.96 B sec^{-1}

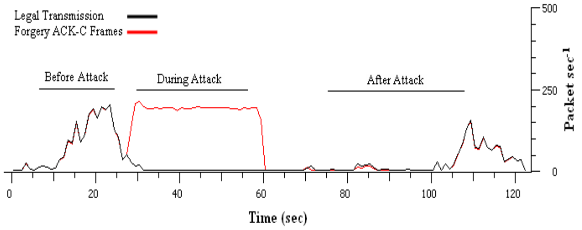

Fig. 8: Virtual carrier sense attack over wireless client using ACK flooding

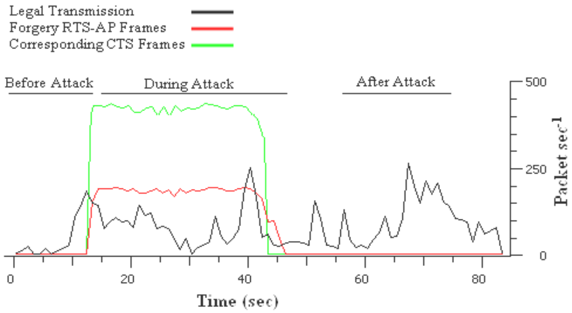

Fig. 9: Virtual carrier sense attack over access point using RTS flooding

As the results show during this attack the wireless network became almost shut down for the victim and it was unable to make any communication. Therefore this attack has a great effect on the performance of the wireless network in term of transmission rate.

Experiment 3: Transmission rate measuring for VCSF-RTS-AP: For this experiment we turned off the RTS/CTS mechanism in all wireless stations to investigate their behavior in case of receiving this type of frame. Then we made our forgery RTS control frame and injected it to the access point of the tested wireless network. The result of the network performance is shown in Fig. 9 before, during and after the VCSF-RTS-AP attack.

As we can see in Fig. 9, the attack duration is 34 sec which started from 13 sec till 47 sec. The results of measured transmission rate in this experiment are as follow:

- Average transmission rate of WLAN before VCSF-RTS-AP = 9380.144 B sec^{-1}
- Average transmission rate of WLAN during VCSF-RTS-AP = 5464.846 B sec^{-1}

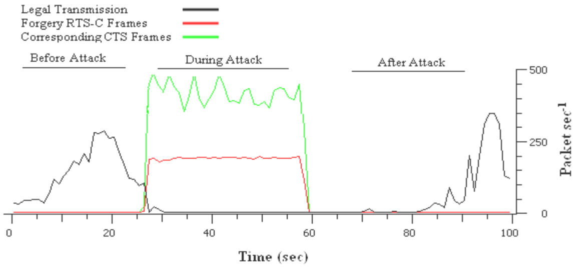

Fig. 10: Virtual carrier sense attack over wireless client using RTS flooding

As we can see from the result, this attack has a less effect on the performance of the network. During this experiments although we injected our forgery frame continually with the maximum duration value, but still all the clients had ability to continue their communication but a little slower. As we can see from Fig. 9, we just injected our RTS forgery to the victim, but there are huge numbers of CTS response that the victim has sent to the attacker. We observed that the amounts of these legal CTS responses were much more than the number of RTS transmitted by the attacker. This causes the network becomes much busier by unwanted packets which makes the attack more effective.

Experiment 4: Transmission rate measuring for VCSF-RTS-C: For this experiment we injected our forgery RTS to a specific client on the wireless network. The result of the network performance of the victim is shown in Fig. 10 before, during and after the attack.

As we can see in Fig. 10, the attack duration is 33 sec which started from 26 sec till 59 sec. We measured the transmission rate for this experiment and the results are as follow:

- Average transmission rate of the victim before VCSF-RTS-C = 3547.284 B sec^{-1}
- Average transmission rate of the victim during VCSF-RTS-C = 9.185 B sec^{-1}

The attack causes the client drops its network connection and has no longer access to the access point until end of the attack period when the attacker makes its resources free to communicate.

Experiment 5: Transmission rate measuring for VCSF-CTS-AP: For this experiment we made a CTS forgery which was injected to the victim access point. The result of the attack is shown in Fig. 11.

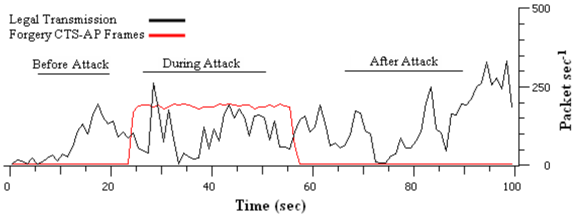

Fig. 11: Virtual carrier sense attack over access point using CTS flooding

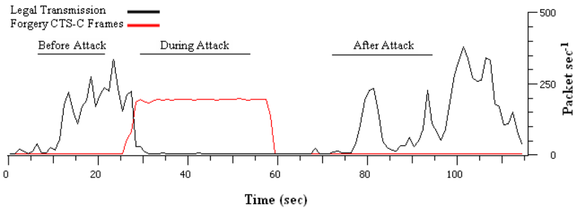

Fig. 12: Virtual carrier sense attack over wireless client using CTS flooding

As we can see from Fig. 11, the attack duration is 33 sec which started from 24 till 57 sec. The transmission rate of the wireless network is measured as follow:

- Average transmission rate of WLAN before VCSF-CTS-AP = 4151.952 B sec^{-1}
- Average transmission rate of WLAN during VCSF-CTS-AP = 3961.429 B sec^{-1}

Again as we expected, the effect of this attack is less. During this experiment we observed that all wireless client connected to the victim access point were able to keep their communication but a little slower because of an increase in the number of forgery frames injected to the network during the attack period.

Experiment 6: Transmission rate measuring for VCSF-CTS-C: In this experiment we injected our forgery CTS frames to a specific wireless client to measure any changes in transmission rate of the victim client. The result of the attacks is shown in Fig. 12 before, during and after the attack.

As we can see from Fig. 12, the attack duration is 33 sec which started from 26 till 59 sec. The results of the transmission rate for the wireless client are measured as follow:

- Average transmission rate of the victim before VCSF-CTS-C = 4959.887 B sec^{-1}
- Average transmission rate of the victim during VCSF-CTS-C = 44.740B sec^{-1}

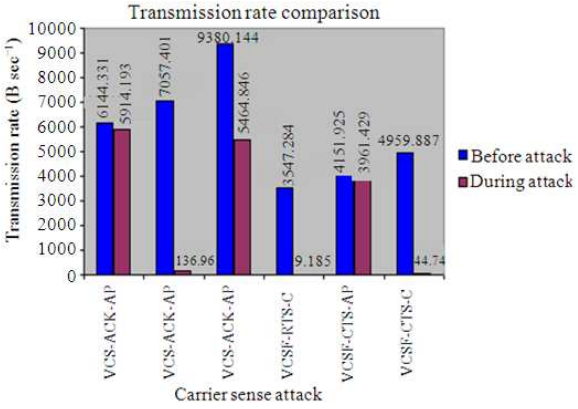

Fig. 13: Comparison results of WLAN virtual carrier sense attacks

As the results show this attack has a direct effect on the victim. The attacker has successfully made the wireless client completely busy with large amount of unwanted frames and consequently provided total inability for the client to keep normal communication.

A summarized comparative result is shown in Fig. 13.

CONCLUSION

In this study we implemented several experiments to show the influence of the virtual carrier sense attacks on the performance of the wireless network in term of transmission rate. We concluded that implementation of the virtual carrier sense attacks on clients has more effect than on the access point. As all the results show, during the attacks on the victim client, transmission rate extremely degraded which makes any communication for the client impossible. Also we concluded from the results that, the attack over virtual carrier sense by using RTS frames makes the media busier which makes the attack more effective than the other type of control frames. This is because IEEE 802.11 standard defines to reply by CTS to a RTS frame to complete the process even this mechanism is not active in the wireless network. Therefore the corresponding CTS frames must be transmitted to response to the related RTS frames which provide more overhead to the network under attack and makes the attack more efficient.

REFERENCES

1. Malekzadeh, M., A. Azim, D. Jalil and S. Shamala, 2008. An experimental evaluation of DoS attack and its impact on throughput of IEEE 802.11 wireless networks. Int. J. Comput. Sci. Network Secur., 8: 1-5. http://paper.ijcsns.org/07_book/200808/20080801.pdf

2. IEEE Computer Society, 1999. Wireless LAN Medium Access Control and Physical layer Specification.
3. Gast, M., 2002. 802.11 Wireless Networks: The Definitive Guide. O'Reilly Publisher, pp: 70-76.
4. Bellardo, J. and S. Savage, 2003. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. Proceedings of the 12th USENIX Security Symposium, Aug. 4-8, Washington DC., USA., pp: 2-2. http://portal.acm.org/citation.cfm?id=1251355
5. Chen, D. *et al*., 2003. Protecting Wireless Networks against a Denial of Service Attack Based on Virtual Jamming. Proceedings of the 9th ACM Annual International Conference on Mobile Computing and Networking, (AICMCN'03), San Diego, CA, USA., pp: 1-2. http://www.sigmobile.org/mobicom/2003/posters/11-Chen.pdf
6. Chen, B. and V. Muthukkumarasamy, 2006. Denial of Service Attacks against 802.11 DCF. School of Information and Communication Technology, Griffith University, Australia. http://www98.griffith.edu.au/dspace/bitstream/10072/12207/1/41331.pdf
7. Sugantha, K. and S. Shanmugavel, 2005. A Statistical Approach to Detect NAV Attack at MAC layer. Proceedings of the International Workshop on Wireless Ad-Hoc Networks, May 25, London, UK., pp: 6. http://ctr.kcl.ac.uk/IWWAN2005/papers/46.pdf
8. Pelechrinis, K. and M. Iliofotou, 2006. Denial of Service Attacks in Wireless Networks: The case of Jammers. Department of Computer Sciense and Engineering University California Riverside. *http://*citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.122.9417&rep=rep1&type=pdf
9. Venkata Krishna P. and N.S.N. Ch Iyengar, 2008. Design of Sequencing Medium Access Control to Improve the Performance of Wireless Networks. J. Comput. Inform. Technol., 16: 81-89. http://cat.inist.fr/?aModele=afficheN&cpsidt=20517386
10. Han, M.K., B. Overstreet and L. Qiu, 2007. Greedy Receivers in IEEE 802.11 hotspots. Proceedings of the 37th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, June 25-28, IEEE Xplore Press, Edinburgh, pp: 471-480. DOI: 10.1109/DSN.2007.53
11. Gupta, N. and P.R. Kumar, 2004. A performance analysis of the 802.11 wireless LAN medium access control. Commun. Inform. Syst., 3: 479-304. http://www.projecteuclid.org/DPubS?service=UI&version=1.0&verb=Display&handle=euclid.cis/1119639800
12. Ye, F., S.T. Sheu, T. Chen and J. Chen Tamkang, 2003. The Impact of RTS Threshold on IEEE 802.11 MAC Protocol. Tamkang J. Sci. Eng., 6: 57-63. http://www2.tku.edu.tw/~tkjse/6-1/6-1-8.pdf