Investigate The Integration of PCF in WLAN to Improve its Performance Against Attackers

Sabbar Insaif Jassim

Technical Institute – Al-Dour

Email: sabbarjan@yahoo.com

Abstract

Wireless network has become the most popular technology among current communities due to cheap hardware, mobility, ease of installation, usage and expandability. Remote system has turned into the most well known innovation among current groups because of modest equipment, portability, simplicity of establishment, use and expandability. There- fore, the performance of WLANs becomes important. Jamming attackers would reduce the performance of wireless network such as decreasing throughput, increasing delay and data dropped ... etc. The IEEE 802.11 standard specifies two different media access con- trol (MAC) mechanisms: *distributed coordination function* (DCF), *point coordination function* (PCF). The IEEE 802.11 standard determines two distinct media get to control (MAC) components: disseminated coordination works (DCF), point coordination work (PCF). PCF achieve higher throughput than DCF, therefore, this study investigates the integration of PCF in WLAN which is attacked by Jammers. This study is done using OPNET Modeler (v14.5). OPNET Modeler (v14.5) is used in this work, because it is the more suitable tool for wireless network. After the simulation was run, the results were collected and showed that PCF gave a good improvement by increasing throughput and decreasing data dropped with an acceptable delay even when the transmission power of Jammer was increased more above the transmission power of computers and PCF also gave a good improvement in throughput and delay when the number of Jammers became two. This would improve the performance of the system.

Key words: jamming, attackers, PCF, OPNET.

تحقيق دمج ال (PCF) لتحسين كفاءة ال (WLAN) ضد هجمات التشويش

صبار نصيف جاسم

المعهد التقني - الدور

الخلاصة

الشبكات اللاسلكية اصبحت من التقنيات الاكثر شهرة بين الاتصالات الحالية وذلك لرخص ثمن مكوناتها المادية، الحركية، وسهولة التركيب والاستخدام و التوسعة . وبالتالي، فإن أداء الشبكات المحلية اللاسلكية اصبح أمرا مهما.

أن تشويش المهاجمين سوف يقلل من أداء الشبكة اللاسلكية مثل تناقص الإنتاجية، وزيادة التأخير الزمني و يزيد من انخفاض البيانات ... الخ ان المعيار IEEE 802.11 يصف اليتين مختلفين للتحكم بالوصول للوسائط (MAC:وظيفة التنسيق الموزعة (DCF) ، وظيفة التنسيق النقطي PCF . (PCF) يحقق إنتاجية أعلى من الالية الاخرى، ولهذا فإن هذه الدراسة تحقق التكامل لل PCF في WLAN والتي تعرضت لهجوم من قبل التشويش . أجريت هذه الدراسة باستخدام (OPNET Modeler (v14.5 لأنه أداة أكثر ملائمة للشبكات اللاسلكية . بعد تشغيل المحاكاة ، تم جمع النتائج و أظهرت أن PCF أعطى تحسن جيد من حيث زيادة الإنتاجية و التقليل من تراجع البيانات مع مستوى مقبول من التأخير الزمني حتى عندما تم زيادة قدرة الارسال للمهاجمين أكثر من قدرة الارسال لأجهزة الكمبيوتر و PCF أيضا أعطى تحسن جيد في الإنتاجية و التأخير الزمني عندما يصبح عدد المهاجمين اثنين. وهذا من شأنه تحسين أداء النظام.

الكلمات المفتاحية: التشويش، المهاجمون، الية ال(PCF)، الاوبنيت.

1-Introduction

An extensive variety of project organizations have realized significant productivity in- crease by circulate mobile data applications utilizing WLAN networks WLAN technolo- gies are better known on account of cost sufficiency, compliance and openness. IEEE 802.11 is projected for best exertion benefits as video conferencing and sound in WLAN. IEEE 802.11 model covers the physical layer and the MAC sub-layer of the OSI network position form for WLANs. The MAC sub-layer characterizes two medium get to coordi- nation works, the required (DCF) and the discretionary (PCF). 802.11 can work both inconflict based DCF mode and dispute free PCF mode [1]. Security is one of the basic things of any remote correspondence arrange because of its nature of the transmission of data wirelessly. Different attacks have been accounted for throughout the last numerous years [2]. This paper presented the effect of jam- ming attacks on WLAN which reduce throughput and increase delay and data dropped and the paper introduced how can PCF will improve the network in terms of increasing the throughput. The study was done and the network was simulated using OPNET Mod- eler (14.5) [3] which is chosen as suitable tool for simulating wireless network due to the complexity of performing these networks in real world.

2-Related work

Many studies had been produced on the security of WLAN against jamming attacks.[4], surveyed on different types of jamming attack and the mit- igation techniques generally used and investigate about the approaches proposed that are considered efficient to survive in a jammed region on various sorts of jamming attack and the moderation methods for the most part utilized and examine about the methodologies recommended that are viewed as proficient to get by in a jammed region [4]. [5] Ali Hamieh and Jalel Ben-Othman considered a particular class of denial of ser- vice attacks called Jamming and propose in this study a new method of detection of such attack by the measurement of error distribution. [6] Tajinderjit Kaur and Sangeeta Sharma presented jamming attack in the systems having hubs with isotropic and directional radio wires. The reproduction comes about demon- strate that is conceivable to minimize the impact of jamming attack by utilizing diverse re- ception apparatus Patterns.

[7] Maulik, R. and Chaki, N. intro- duced a complete survey done on the exceptionally late best in class explore comes about on wormhole attacks and applicable moderation measures.

3-Wireless local area network

Wireless network has turned into the most mainstream innovation among current groups due to cheap hardware, mobility, unlicensed band, portability, ease of installation and usage and expandability. Therefore, the performance of WLANs becomes important. It is outstanding that WLANs give a physical layer multi-rate capacity, and henceforth MAC layer instruments are expected to adventure this ability. This nature of WLAN made it vulnerable to attackers [8]

Wireless networks are more portrayed to purposeful or unexpected dangers than their wired based identical systems since that remote medium can be listened and meddled by non-members, in an on-going logical communication. The remote medium presents nu- merous dangers which can't be effortlessly tended to by the customary security strategies. One noteworthy arrangement of such attacks is denial of service, which is worried with fulfilling client or framework area supports. In wireless network resistances like cryptog-raphy, pass-express sharing and so on, can be overcome by a basic denial of service attack that can shade the entire system [4].

4-Jamming attackers

[9] characterized a Jammer to be a substance who is deliber- ately attempting to meddle with the physical transmission and gathering of remote in- terchanges [2]. Jamming is an extraordinary class of denial of service attacks utilized as a part of wireless networks, where an attacker affronts the MAC protocol and transmits on the mutual channel; either consistently or occasionally to focus on all or some correspondence, separately [4]. The target of a jammer is to meddle with authentic wireless communications. A jammer can accomplish this objective by either keeping a genuine movement source from conveying a package, or by keeping the gathering of true blue bundles [5]. Fig. 1 demonstrates a jamming situation in wireless network, where the red range denotes the jammed area [4]. Jamming attacks would reduce the performance of the system by reducing throughput and increasing delay and data dropped. Many studies focus on improving the performance of system against jammers.

It is outstanding that WLANs give a physical layer multi-rate ability, and subsequently MAC layer components are expected to attempt this capacity [8] Zhu, and Cao,2004.

5-Point coordination function

The IEEE 802.11 standard indicates two distinctive MAC systems: one is called (DCF), in view of CSMA/CA; the other is called (PCF), in view of surveying. DCF is the fundamen- tal MAC component while PCF is based on top of DCF and gives conflict free media get to. PCF can accomplish higher throughput than the dispute

based DCF and give ensured benefit because of the way of PCF conflict free and this is vital for ongoing applications. PCF could likewise be utilized for non-real-time services [8]. In or- der to control the access to the shared wireless medium and eliminate contention among wireless stations, PCF adopts a poll-and-response protocol. It makes use of the PIFS to seize and maintain control of the medium [10].

The center of the IEEE 802.11 standard is the BSS. A BSS is a gathering of station's organized by DCF and PCF. It is additionally considered as the scope region gave by a solitary AP. The AP and mobile stations can convey utilizing the radio channel with an adequate least quality. The region secured by BSS is known as BSA. PCF underpins time bound support of let stations have conflict free access to the wireless medium, facilitated by the PC. The PCF gives synchronous administration that fundamentally actualizes surveying based get to. It has a higher need than the DCF [1].

6-Opnet Modeler

OPNET [3] is an examination arranged network system simulation tool. It gives a complete improvement environment to displaying and re-enactment of sent wired and remote systems. OPNET Modeler empowers clients to make tweaked models and to reproduce different system situations [11]

OPNET is an abnormal state occasion based system level simulation instrument(Jarmo Prokkola):

•Simulation works at "parcel level"

•Originally worked for the reproduction of settled systems

•OPNET contains an immense library of precise models of financially.

(Figures and graphics for OPNET is shown as in Figures parts)

7-Model Description

The simulation setup based on OPNET Modeller of the proposed system consists of three cases. Each case consists of three scenarios. The first scenario consists of a number of computers connected wirelessly to AP which is connected to switch to the server. Then the jammer applied to the system in the second scenario which reduce throughput and increase delay and data dropped. The proposed method was to enable PCF of two selected guard nodes and the access point of the system in order to improve the performance of the system by increasing throughput which reduced by Jammer and decreasing delay and data dropped that are increased by the Jammer as will be shown and discussed in the following sections.

7.1 Case 1

The transmission power of workstations (computers) = 0.005 W

The transmission power of Jammer = 0.001 W

The network topology of the proposed network contains the following:

- Wireless stations: wlan_wkstn_adv with Direct Sequence Physical characteristics and 11 Mbps Data rate.
- Access Point (AP): wlan_ethernet_slip4_adv with with Direct Sequence Physical characteristics and 11 Mbps Data rate.
- The Switch: ethernet32_switch.
- The Server: ethernet_server.
- Jammers: (jam_pulsed), the Jammers in all scenarios have 2,401 base band frequency and 22,000 bandwidth.
- Links: the setting of links in all scenarios was 100 BaseT.

7.1.1 Scenario 1: WLAN without jammers

This scenario consists of four PCs (wlan_wkstn_adv) connected wirelessly to AP (wlan_ethernet_slip4_adv) which is associated with the switch (ethernet32_switch) - (ethernet_server) as appeared in Fig. 2.

7.1.2 Scenario 2: WLAN with one jammer

This scenario consists of four PCs (wlan_wkstn_adv) connected wirelessly to AP (wlan_ethernet_slip4_adv) which is associated with the switch (ethernet32_switch) - (ethernet_server). The jammer (jam_pulsed) applied in this scenario. The transmission power of Jammer is 0.001 W. This scenario is shown in Fig. 3.

7.1.3 Scenario 3: WLAN with one jammer with PCF

This scenario consists of four PCs (wlan_wkstn_adv) connected wirelessly to AP (wlan_ethernet_slip4_adv) which is associated with the switch (ethernet32_switch) - (ethernet_server). The jammer (jam_pulsed) applied in this scenario and PCF enabled in AP with two selected guard nodes (shown in oval shape performed in Fig.4).

7.2 Case 2

The transmission power of workstations (computers) = 0.005 W

The transmission power of Jammer = 0.01 W

Scenario 4, Scenario 5 and Scenario 6 were the same as Scenario 1, Scenario 2 and Scenario 3 respectively as shown in Fig. 2 , Fig. 3 and Fig. 4 but with Jammer's transmission power = 0.01W.

7.3 Case 3

The transmission power of workstations (computers) = 0.005 W
The transmission power of Jammer = 0.001 W
The number of Jammers had been doubled (No. Of Jammers = 2).
Scenario 7, Scenario 8 and Scenario 9 shown in Fig. 2, Fig. 5 and Fig. 6 these scenarios were the same as Scenario 1, Scenario 2 and Scenario 3 respectively but with number of Jammers was two.

After nine scenarios designed in the proposed framework, Discrete Event Statistics were decided for every scenario. The application designed in this system was video con- ferencing. The simulation was keep running for 20 minutes. What's more, the outcomes were gathered to be discussed as coming.

8-Results

Case 1: The gathered outcomes, when the power transmitted was 0.005 W for the workstation and 0.001 W for Jammer, were as below:

1- **Throughput:** Represents the total number of bits (in bits/sec) forwarded from wireless LAN layers to higher layers in all WLAN nodes of the network. The throughput for three scenarios (WLAN without Jammers, WLAN with One Jammer, WLAN with One Jammer with enabled PCF) shown in Fig. 7.

The throughput for the network without Jammer was 1,307,207 bit/sec. The Jammer reduced the throughput to 896,304 bits/sec which affect the performance of the network. The PCF which was enabled in the two guard nodes and the AP would improve the performance and increase throughput to 2,788,223 bit/sec.

2- **Delay:** Represents the end to end delay of all the packets received by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. Speaks to the end to end delay of the considerable number of parcels got by the wireless LAN MACs of all WLAN nodes in the network and forwarded to the higher layer. The delay for three scenarios (WLAN without Jammers, WLAN with One Jammer, WLAN with One Jammer with enabled PCF) shown in Fig. 8.

The existence of Jammer in the network increased the delay from 0.324 bits to 0.413 bits. The PCF which was enabled in the two guard nodes and the AP increased the delay to 3.52 bits. This increase in delay was acceptable compared with the improvement caused by PCF.

3- **Data dropped**: The aggregate size of higher layer information parcels (in bit/sec) dropped by all the WLAN MACs in the network due to: a) full higher layer data buffer, or b) the size of the higher layer packet, which is greater than the maximum allowed data size defined in the IEEE 802.11 standard. The data dropped for three scenarios (WLAN without Jammers, WLAN with One Jammer, WLAN with One Jammer with enabled PCF) shown in Fig. 9.

As shown in an above figure, the Jammer in the network increased the data that were dropped due to buffer overflow from 12,685,082 bits/sec to 13,090,744 bits/sec. The PCF which was enabled in the two guard nodes and the AP reduced the data dropped to 10,867,588 bit/sec which is good improvement for the proposed network.
Case 2:The gathered outcomes, when the power transmitted was 0.005 W for the workstation and 0.01 W for Jammer, were as below:

1- **Throughput:** The throughput for three scenarios (WLAN without Jammers, WLAN with One Jammer, WLAN with One Jammer with enabled PCF) shown in Fig. 10.

Jammers would largely reduced throughput of the network from 1,307,025 bits/sec to 871,114 bits/sec. The PCF which was enabled in the two guard nodes and the AP increased the throughput to 1,016,269 bits/sec.

2- **Delay:** The delay for three scenarios (WLAN without Jammers, WLAN with One Jammer, WLAN with One Jammer with enabled PCF) shown in Fig. 11.

Jammer would increased the delay from 0.3246 sec to 0.5068 sec and the PCF which was enabled in the two guard nodes and the AP decreased the delay to 03914 sec which is a good improvement.

3- **Data dropped**: The data dropped for three scenarios (WLAN without Jammers, WLAN with One Jammer, WLAN with One Jammer with enabled PCF) shown in Fig. 12.

Case 3: The collected results when the number of jammers was two as follows:

1- **Throughput:** the throughput when the number of Jammers was two for three scenarios (WLAN without Jammers, WLAN with Two Jammers, WLAN with Two Jammers with enabled PCF) shown in Fig.13

When the two Jammers applied to the network, the throughput was also decreased from 1,307,025 bits/sec to 886,102 bits/sec. PCF also improve the performance of the network by increasing throughput to 1,542,884 bits/sec which is a good improvement in spite of the existence of two Jammers.

2- **Delay:** the delay when the number of Jammers was two for three scenarios (WLAN without Jammers, WLAN with Two Jammers, WLAN with Two Jammers with enabled PCF) shown in Fig. 14.

Two Jammers increased the delay of the network from 0.324 sec to 0.416 sec. The PCF enabled in the two selected guard nodes and AP would improve the network by decreasing delay to 0.153 sec. This is very good improvement for the network by decreasing the delay of network.

3- **Data dropped:** the data dropped when the number of Jammers was two for three scenarios (WLAN without Jammers, WLAN with Two Jammers, WLAN with Two Jammers with enabled PCF) shown in Fig.15.

Also, PCF enabled in the two selected guard nodes and the AP would improve the network by decreased data that was dropped in the existence of Jammers from 13,100,299 bits/sec to 13,384,721 bits/sec.

9- Conclusions

Wireless networks have picked up a ton of consideration and turn into the most well known innovation among current communities. Because of the way of radio transmission and the common medium access between the stations, this makes WLAN helpless against attacks. Jammer is a unique classification of DoS attacks which is utilized as a part of wireless networks. Jammer will reduce the performance of the network by decreasing the throughput and increasing delay and data dropped. The IEEE 802.11 standard specifies two different MAC mechanisms DCF and PCF. PCF can accomplish higher throughput than the conflict based DCF and give ensured benefit due to the nature of PCF contention-free and this is important for real-time applications. The proposed network in this study would enable Point Coordinator Functionality (PCF) in the two guard nodes and the AP. three cases were taken in this study, and the simulation was done using OPNET Modeler (14.5) which was proven to be a suitable simulation tool for the wireless network. The results showed that PCF would increase throughput which was reduced by the Jammer attacker and decrease delay which was decreased by the Jammers as shown in Figs. (7, 8 and 9). This improvement was achieved even when the transmission power of the Jammer was increased from 0.001 W to 0.01 W. The PCF also decreased data dropped which was increased by the Jammer. The increasing in throughput and decreasing in data dropped was to the detriment of increasing the delay yet this is an adequate for this network as appeared in Figs. (10, 11 and 12). Enable of PCF would give a good improvement in throughput and delay when the number of Jammers was increased to two by increasing the throughput and decreasing the delay as shown in Figs. (13, 14 and 15). The same effect of PCF would be achieved to improve the performance of the network when the transmission power was increased more and more. More station (Wireless Nodes) can be taken for more studies with effectively improvement on the performance of system. PCF was good functionality to improve network which is attacked by Jammers with different number of wireless stations and different levels of Jammer's transmission power. Future works can enable PCF in Ad-Hoc network with mobile ad hoc routing protocols to improve this kind of network against Jammers.

10- Reffrences

[1] A. R., V. Vityanathan, and C. P. R, "Wlan qos issues and ieee 802.11e qos enhancement," *International Journal of Computer Theory and Engineering*, vol. 2, no. 1, pp.
143–149, 2010.

[2] P. K. and I. M. S. V. Krishnamurthy, "Denial of service attacks in wireless networks: The case of jammers," *Communications Surveys & Tutorials, IEEE*, vol. 13, no. 2, pp. 1–16, 2011.

[3] "Opnet official website." [Online]. Available: www.opnet.com.

[4] A. F., Z. A., M. S., and H. K, "Survey on survival approaches in wireless network against jamming attack," *Journal of Theoretical and Applied Information Technol- ogy*, vol. 30, no. 1, pp. 55–67, 2011.

[5] H. A. B.-O. J, "Detection of jamming attacks in wireless ad hoc networks using error distribution," *IEEE Communications Society subject*, 2009, matter experts for publication in the IEEE ICC proceedin.

[6] K. T. and S. S., "Mitigating the impact of jamming attack by using antenna patterns in manet," *VSRD IJCS & IT*, vol. 2, no. 6, pp. 437–445, 2012.

[7] K. B., N. H., N. Y., K. N, and J. A, "A survey of routing attacks in mobile ad hoc network," *IEEE Wireless Communications*, vol. 14, no. 5, pp. 85–91, 2007.

[8] Z. H. and C. G., "On improving the performance of ieee 802.11 with relay-enabled pcf." Mobile Networks and Applications 9 ©Kluwer Academic Publishers, 2004, pp. 423–434.

[9] X. W., T. W., Z. Y., and undefined Wood T, "The feasibility of launching and detecting jamming attacks in wireless networks." in MobiHoc Urbana-Champaign, USA, 2005, pp. 46–57.

[10] D. Q. A., S. C. B, A. S. C, and K. G. Shin, "Energy-efficient pcf operation of ieee 802.11a wlans via transmit power control," *Computer Networks 42 Elsevier*, pp. 39–54, 2003.

[11] M. G. and S. A., "Performance evaluation of wifi and wimax using opnet, ijarcse," *IJARCSE*, vol. 3, no. 6, pp. 571–579, 2013.

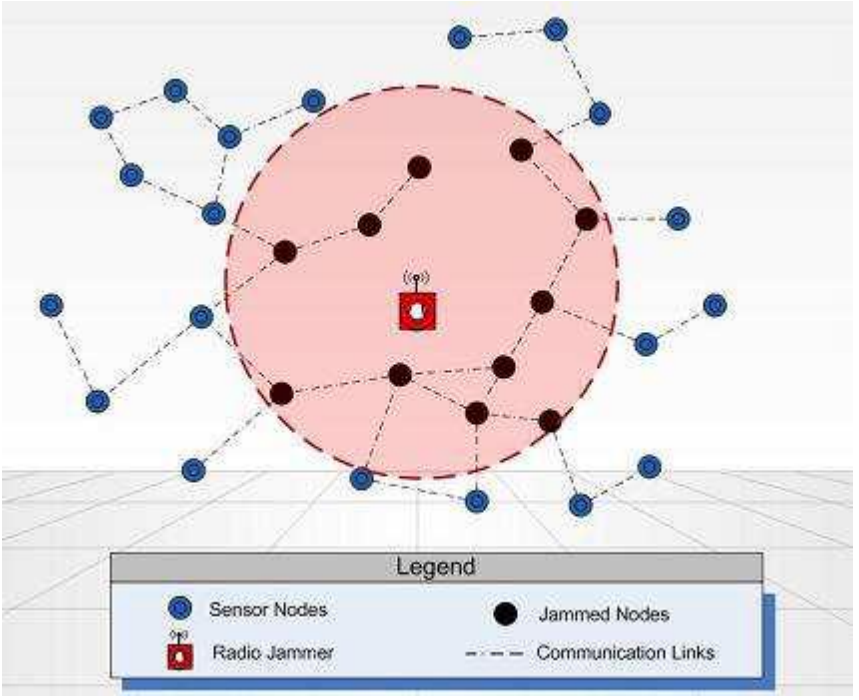

Figure 1 Jammed scenario

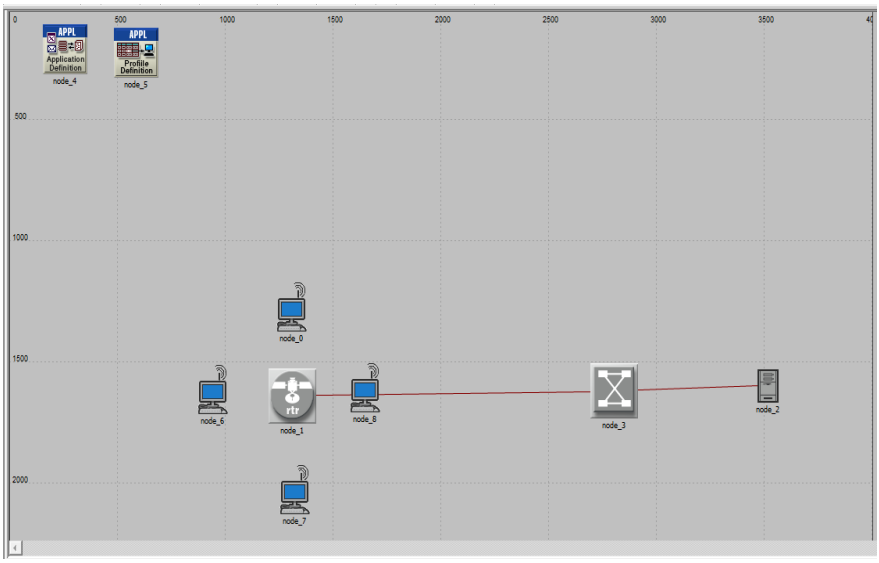

Figure 2 WLAN without jammers

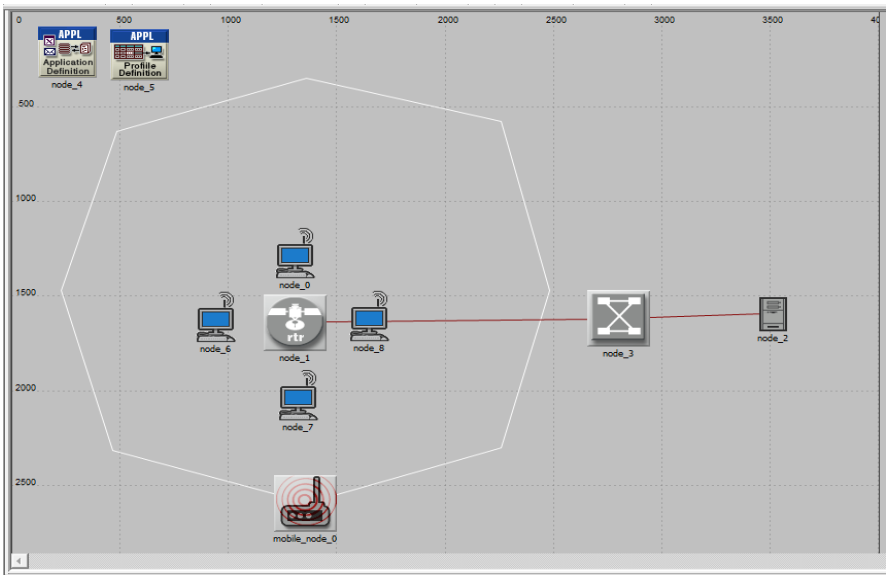

Figure 3. WLAN with one jammer

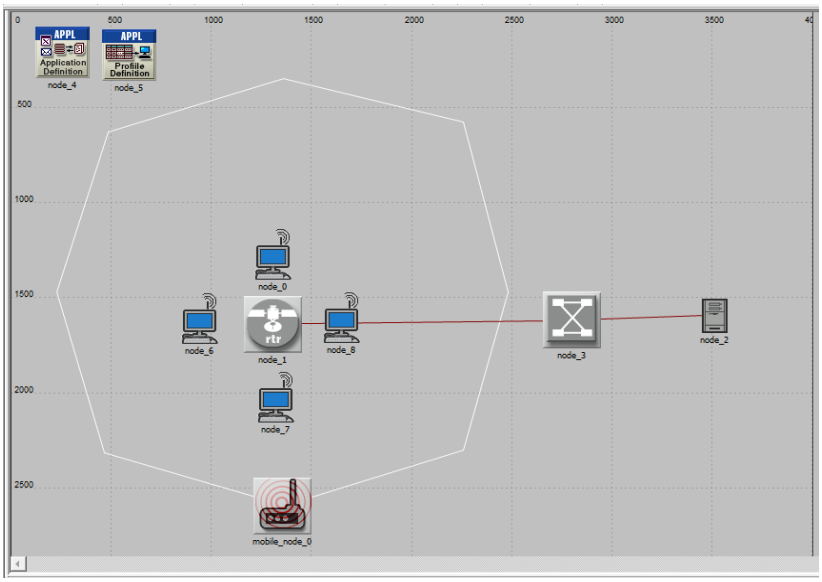

Figure 4. WLAN with One Jammer with PCF

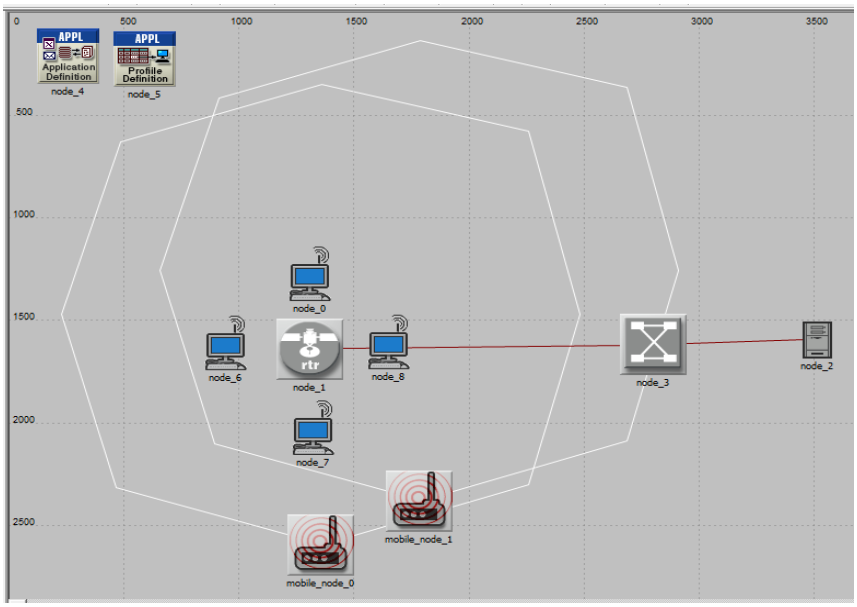

Figure 5. WLAN with Two Jammers

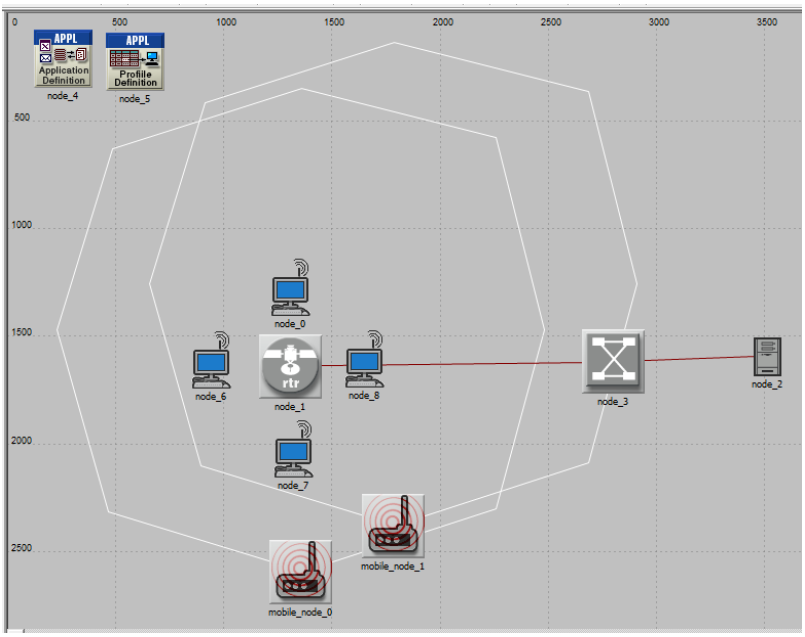

Figure 6. WLAN with Two Jammers with PCF

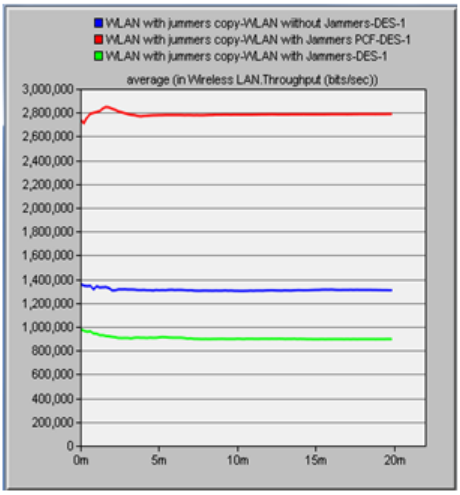

Figure 7. Throughput

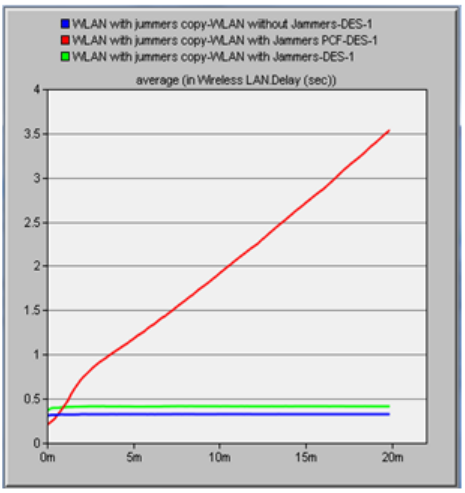

Figure 8. Delay

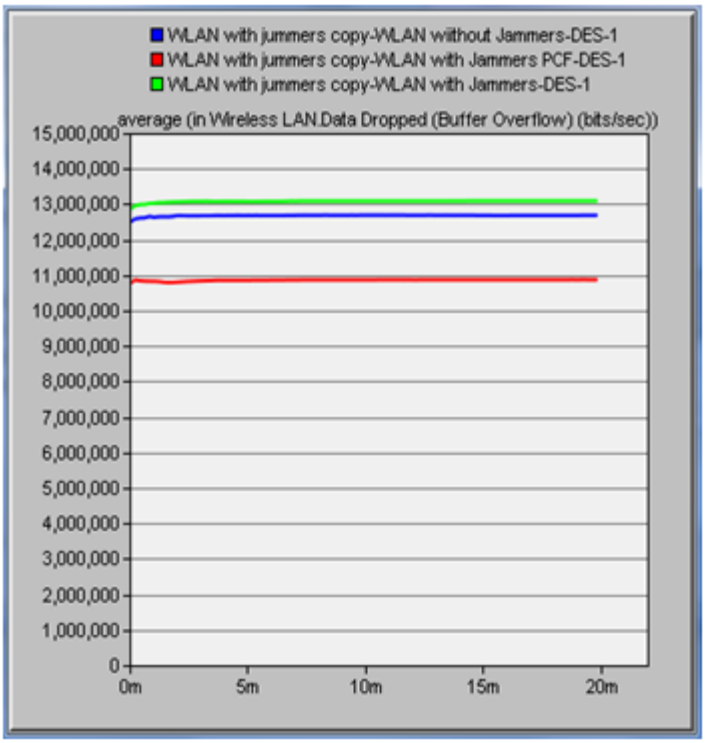

Figure 9. Data dropped

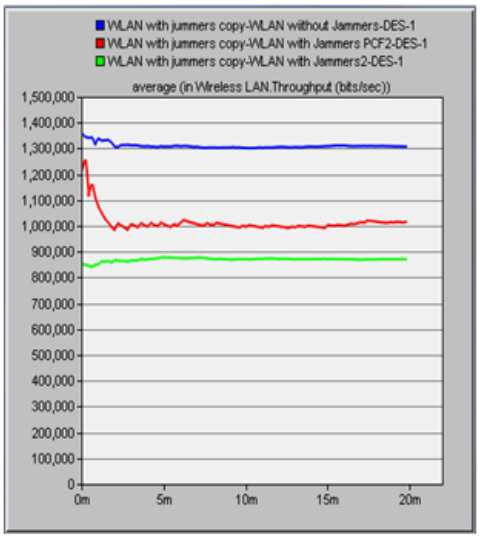

Figure 10. Throughput

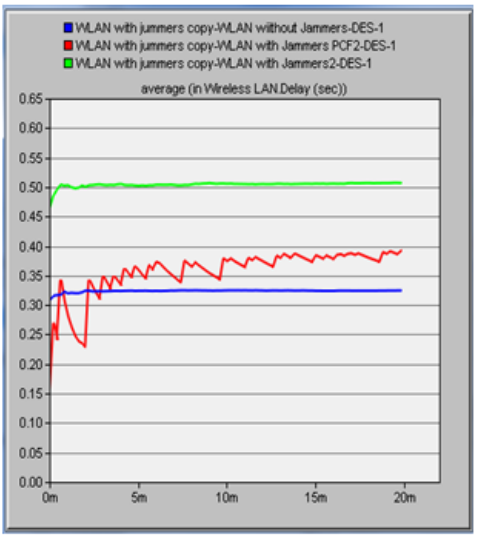

Figure 11. Delay

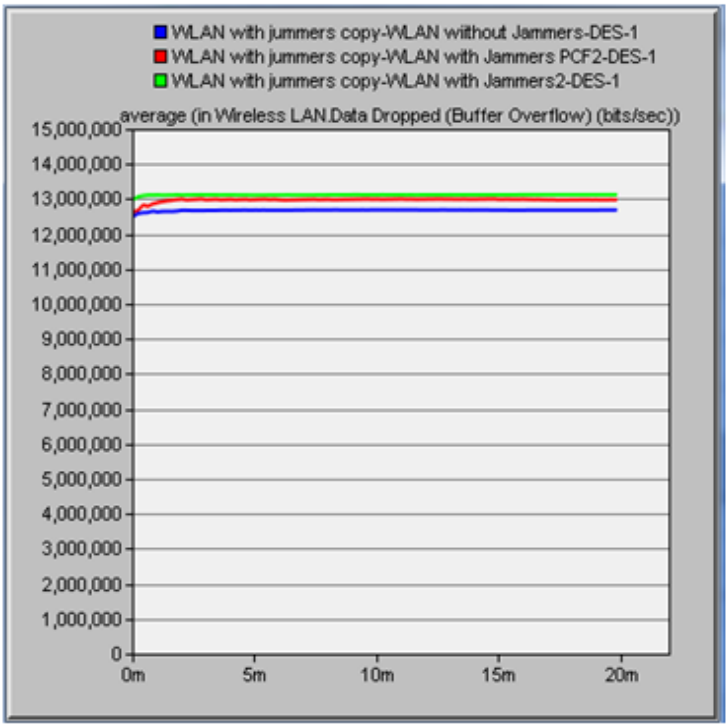

Figure 12. Data dropped

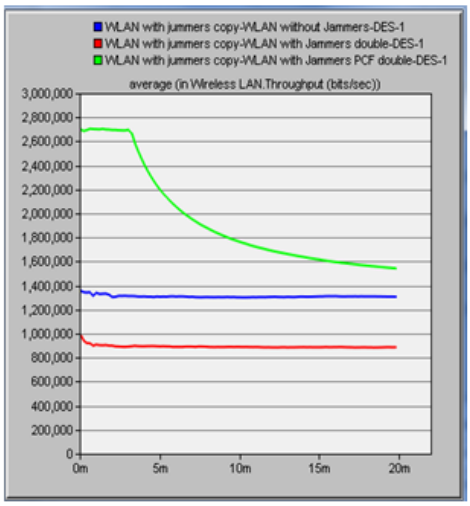

Figure 13. Throughput

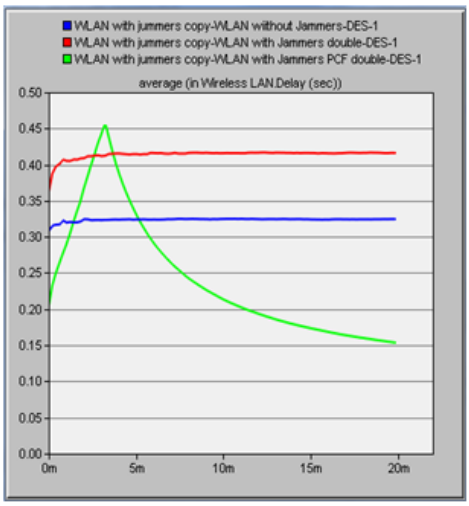

Figure 14. Delay

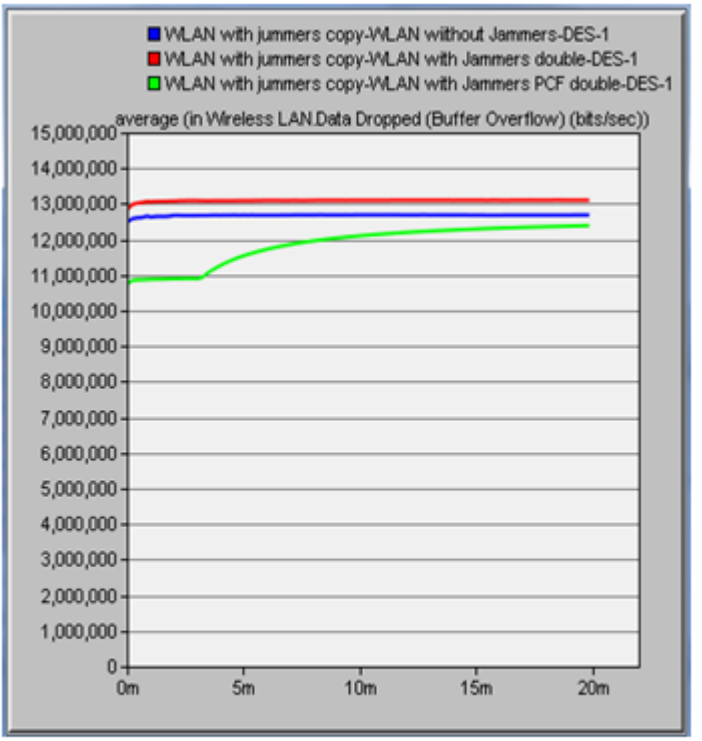

Figure 15. Data dropped