Wireless Local Area Network VLAN Investigation and Enhancement Using Routing Algorithms

Siddeeq Y. Ameen, Shayma Wail Nourildean

Abstract— Wireless LANs, WLANs, are vulnerable and witnessed numerous types of threats. These can be avoided via several security technologies such as WEP, 802.11i and WPA. These technologies have draw backs on performance and an alternative approaches that might have less impact on performance is the Virtual Local Area Network (VLAN). The paper introduces the integration of VLAN into WLAN system. The use of VLAN will provide the security to the system by isolating the access and grouped in such away that avoid any group from accessing unauthorized station in other group. OPNET Modeler (14.5) was used as a simulation program for this study. In the investigation, the effect of VLAN technology on decreasing the traffic in the system of the WLAN has been investigated. In the investigation also the delay, throughput, traffic sent and received with Email and Web browsing applications have been computed and compared with the conventional case of no VLAN. The results show that use of VLAN greatly reduces the throughput. This problem has been resolved via the use of routing algorithms, AODV, OLSR and DSR. The results of employment of routing algorithms with VLAN over WLAN have been investigated the enhancement in throughput has been achieved.

Keywords- WLAN, VLAN, AODV, OLSR, DSR.

I. INTRODUCTION

Wireless Local Area Networks (WLANs) are one of the desirable way of communication because of the flexibility that offered. WLANs allow computers to communicate with each other with a speed very close to that of wired LANs. However, the cost of these benefits is the network security threats [1]. WLANs have more risks and vulnerabilities than that in the conventional wired network. These security threats may be passive attacks or active attacks. There are also other threats such as loss of confidentiality, loss of integrity and loss of network availability in WLANs [1]. These security weaknesses of WLANs suggest the employment of security services in WLANs. Security services include privacy, integrity, availability, nonrepudation and access control. These services can be accomplished via mechanisms such as cryptography and authentication. VLAN is one of the security mechanisms that can solve the authentication problem. VLANs also offer network operators flexibility for specifying management and security policies within an enterprise and allow operators to implement some level of isolation by separating hosts into different broadcast domains [2].

Manuscript received December, 2013

Prof. Siddeeq Y. Ameen, Department of Computer and Information Engineering, University of Mosul Mosul, Iraq.

Shayma Wail Nourildean, Assistant Lecturer, Technical Institute – Al-Dour Tikrit, Iraq.

The objective of this paper as to study the performance of VLAN in wireless Local area Network The performance of the system was studied using OPNET Modeler v14.5. Throughput, delay, load, traffic sent and received were measured to study the performance of the system with and without VLAN. The effect of routing algorithms such as AODV, OLSR and DSR on the performance of WLAN employing VLAN will also be investigated.

II. WIRELESS LAN TECHNOLOGY AND VIRTUAL LOCAL AREA NETWORK

Wireless communication that contains several different portable and mobile devices without the need for wire connectivity has witnessed exponential growth in the recent years. Furthermore, the wireless connectivity achieved with fixed base station and moving nodes and devices and for this reason called mobile wireless communication [3]. Thus the interest and growth come from the mobility, portability and flexibility and other features that mobile wireless networks achieve. This has enforced the researchers to realize mobile computing environment with a communication architecture that must be compatible with the current architectures and also takes into account the specific features of mobility and wirelesses [4].

The market now is busy with mobile devices that provide several services and applications. These services as the wired services should be reliable. Many developments to these services have been provided in the recent years, but these developments that make such mobile services attractive require hardware and software development to achieve. The researcher and development companies are working hard in these attractive developments work hard to achieve these requirements, because of their direct impact on the business.

With VLAN, the physical network structure can be configured logically and impendent from the physical structure. It isolates WLANs computers in a manner that provides more security and even better performance. This can be achieved by configuration of VLAN switches and users such that the access to their department networks from a common space as shown in Fig. 1 [5].

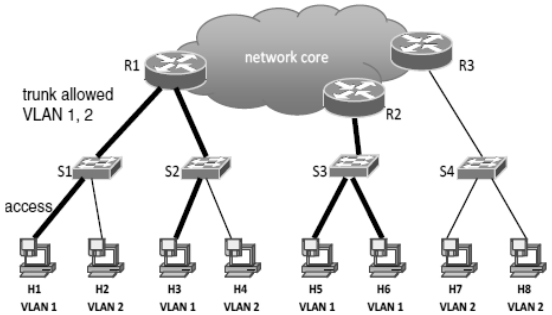


Figure 1. A simple enterprise VLAN setup

Therefore, in VLAN logical connectivity between switch ports can be provided. Devices on a given VLAN can communicate with devices on the same VLAN. This will provide the security required, access control and will

improve the overall network performance, scalability and network management. The performance will be enhanced because VLANs reduce broadcast traffic, enhance traffic control in providing flexibility in locating and relocating devices on IP network [6]. Thus the network administrators can group users according to services that most frequently used. In this aspect, comprehensive monitoring tools are required to allow network administrators to maintain efficient communication paths throughout the switched infrastructure. The latter can be achieved via the use of efficient routing algorithms. Therefore, the research paper will investigate the most efficient routing in wireless network

III. ROUTING IN WIRELESS NETWORKS

Routing protocols might be reactive or proactive protocols. In reactive routing protocols, routing information is not kept by these protocols. Routes are built when the source needed. Route request is sending across the network to achieve this. On the other hand, Proactive routing protocol the route are created and maintained via periodic and event-driven messages. These routing protocols may be classified into distance vector or link state. One of the main types of proactive routing protocol is Optimized Link State Routing (OLSR) [8]. In proactive distance vector protocol, every node maintains a routing table with one route recorded. One of the main problems that may appear with OLSR, is the routing loop which can be avoided with the use of destination sequence number employed by distance vector protocol [8].

This type of protocol uses Multipoint Relay (MPR) as key point in the optimization. The MPRs, is a node that is guaranteed that the message are flooded. This can be achieved by flooding a message to its when retransmitted by the MPRs, will be received by all its two-hop neighbors. Other form of proactive routing protocol is the TBRPF. Shortest path computation in link state for all nodes will require different overhead reduction technique and require bandwidth optimization. This bandwidth optimization can be achieved to part of the tree that is propagated to neighbors [8].

A reactive routing protocol specified by its way to reduce the control traffic messages overheads by maintaining information for active routes only. However, such process will require more time in finding new routes. In such routing protocol, the route between two nodes will be established on the demand only. Dynamic Source Routing (DSR), Ad Hoc On-Demand Distance Vector (AODV), many others are all form of reactive routing protocols. The DSR is a loop-free, source-based and on-demand routing protocol. In such protocol, a route cache is maintained in each. This includes the source routes that have been learned by the node. With DSR, route discovery process is used in the initialization when a source node does not have a valid route to the destination in its route cache. As new routes are learned, the entries in the route cache are continually updated. Source routing is used for packet forwarding. AODV is an enhancement to the DSDV protocol. The AODV attempt to minimize the number of route broadcasts. This can be achieved using on demand establishment, whereas the DSDV maintaining a complete list of routes. In AODV, route discovery is initiated on demand, as achieved in DSR. Having initiated the routes, a route request is then forwarded by the source to the destination [9].

IV. NETWORK SIMULATION

Simulation is an easy way to test of a generated scenario. It is possible to change the network size and node deployment without any costs. Simulation statistic results give the possibility to evaluate the performance of the implemented model and parts of the algorithm. Mistakes of design can be easily fixed in a simulation environment opposed to fixing them in real models.

The OPNET Modeler (v14.5) have been adopted in this paper as a simulation tool to study the network security in the WLAN and how routing algorithm can enhance the performance. OPNET is an event-driven, network simulation tool, which allows an easy implementation of the all model elements The OPNET Modeler environment includes tools for all phases of a study, including model design, simulation, data collection, and data analysis. Packets definition can follow exact protocol specifications. It is easy to deploy network elements in the project editor with all parameters can be easily configured.

A. Simulation Setup

Initially, the simulation setup investigates the WLAN model with and without VLAN to study the performance of VLAN in different scenarios. The setup assumes that there are two servers and two switches that connect two departments. The other parameters used in these scenarios are:

- Three access points: named (wireless_ethernet_slip4_router), which had two Ethernet interface and 4 serial line.
- Numbers of workstations: named (wlan_wkstn) which represent clients that communicate with internet. Two cases have been considered 15 and 30 workstations.
- Two VLAN switch: named (Ethernet_16 switch) which represent switch with 16 ports configuration.
- Two server: named (Ethernet Server) which represents point to point server to represent two departments.
- Links: named (100Base-T) to connect the parameters used for the modeled system.

Profile and application configuration: to define the application of the system.

B. Scenario 1 (No VLAN)

In this scenario, the system consists of number of workstations connected wirelessly to three access points which connected to two switches by (100Base-T) connected to two servers. This scenario was shown in Fig.2. In this figure, any workstation (PC1, PC2, …… PC15) can communicate with any of the two servers through the two switches at any time which result in high throughput (number of bits transmitted per second).

C. Scenario 2 (VLAN)

In this scenario, the system is divided into two VLANs (VLAN10, VLAN20). PC1, PC2,…… and PC5) connected wirelessly to Access Point 1 and the workstations (PC6, PC7, …. PC10) connected wirelessly to Access Point 2 and the workstations (PC11, PC12, …. PC15) connected wirelessly to Access Point 3. The access points 1 and 2 are connected to the switch1 by (100Base-T). The access point 3 is connected to the switch2 by (100Base-T). Switch 1 connected by (100Base-T) to Server AA and Switch 2 connected by (100Base-T) to Server BB. This scenario was shown in Fig.3.

The clients and servers are connected by the two VLAN switches with access ports. The PVID of these ports identify the VLAN association of these connected end-nodes. The switches connected to each other with trunk ports which support both VLAN 10 and VLAN20. The communication between the PC's and servers corresponds to VLAN 10 and VLAN 20 is as shown in Fig. 4 and Fig. 5. The (100Base-T)

link between switch1 and switch2 acts as Trunk Port in the VLAN system. In this scenario (VLAN), any PC could not communicate to any server at any time. In Fig.5, (dotted line) shows the communication between PC's in VLAN 10 to the switches and servers. Access Point 1 forward packets from PC's VLAN 10 to switch1 to (server VLAN 10) and Access Point 3 forward packets from PC's VLAN 10 to Switch2 to Switch1 to server VLAN10. In Fig.6, the dotted line shows the communication between PC's in VLAN 20 to switches and server.

In Fig. 5 the Access Point 2 forward packets from PC's VLAN 20 to Switch1 to Switch2 to and server. DES (Discrete Event Statistics) were chosen for the four scenarios () in terms of many parameters according to this study. After choosing the statistics, the simulation was run for 30 minutes and the results were collected.

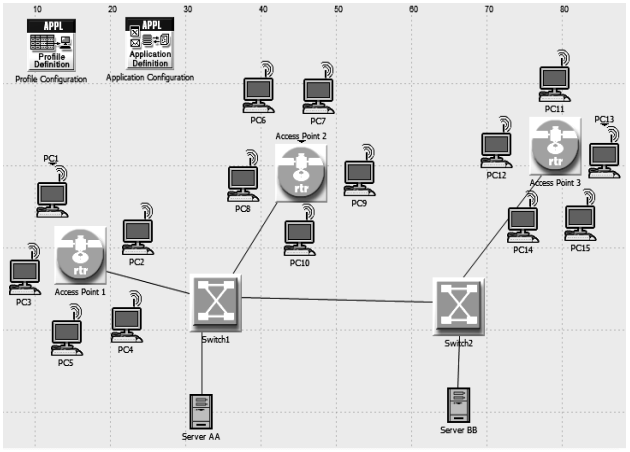


Figure 2. No. VLAN scenario 1 case.

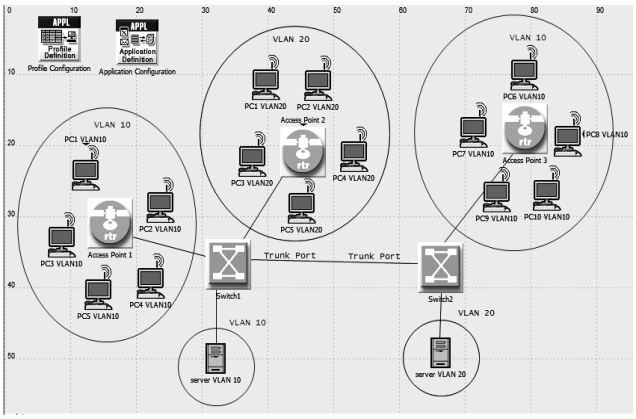
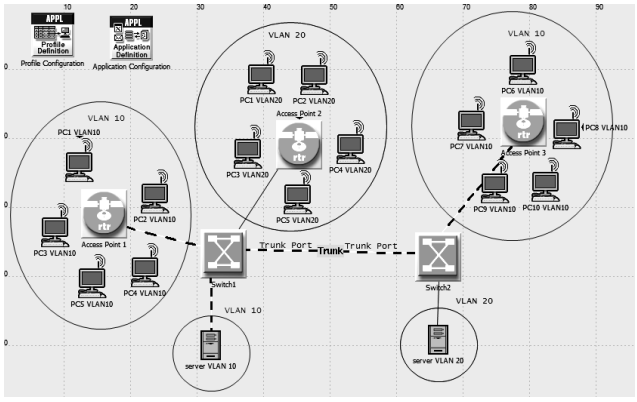


Figure 3. VLAN scenario 2 case.



V. SIMULATION RESULTS AND ASSESSMENTS

The initial investigation measures the throughput and delay in the wireless network of 15PCs shown in Figs. 2 and Fig. 3 with and without VLAN. The results of such investigation are shown in Fig. 6. and Fig. 7, respectively for delay and throughput variation.

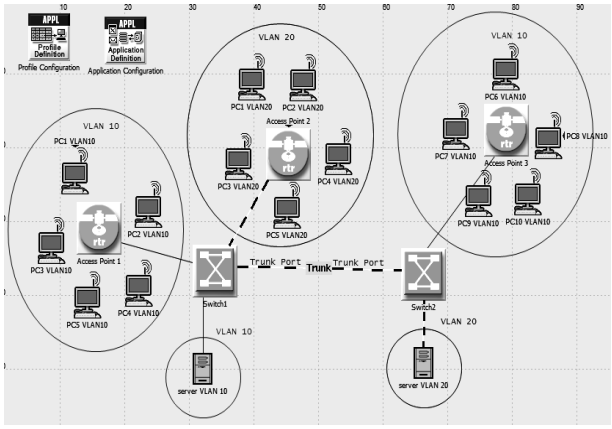


Figure 4. Communication between PC's in VLAN 20.

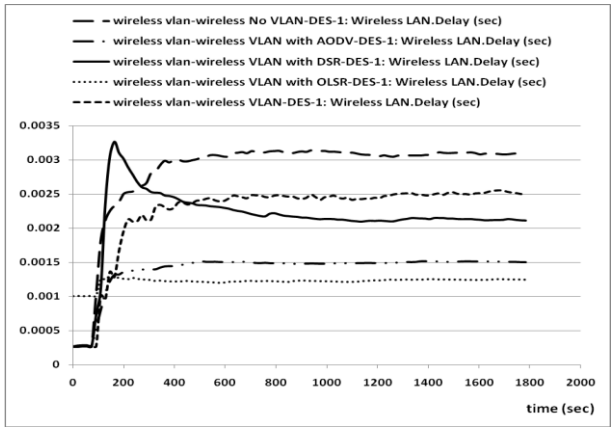


Figure 5. Delay for the case with and without VLAN scenarios.

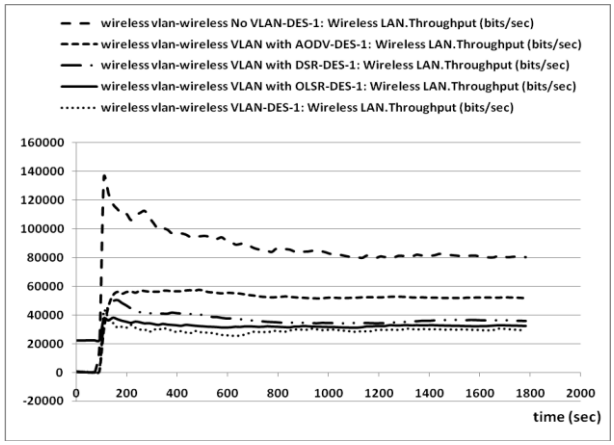


Figure 6. Throughput for the case with and without VLAN scenarios.

It is clear from Fig. 6 and Fig. 7 that the delay has been reduced with the use of VLAN, whereas the throughput also reduced. The latter is the major draw back of using VLAN in WLAN. Therefore, an enhancement for the usage of VLAN has been suggested via the adoption of various routing protocols AODV, OLSR and DSR.

The results of usage of routing protocols shown in Figs. 6 shows that delay can be further reduced and it depends on the routing protocol type. The highest reduction in delay can be achieved with usage of OLSR with the VLAN. The results also show that an improvement in throughput can be achieved by employing routing protocol. The results shown in Fig. 7 suggest that the AODV routing protocol gives the highest improvement in throughput with usage of VLAN.

Extra investigation to show the effect of the number of workstations on the performance of WLAN employing VLAN has also being conducted. The results of such investigation is as shown in Fig. 8 and Fig. 9 for the delay and throughput respectively. The result shows that the AODV gives higher throughput as the number of station is increased from 15 to 30 workstation, whereas the OLSR gives the least delay as the number of workstation are increased from 15 to 30.

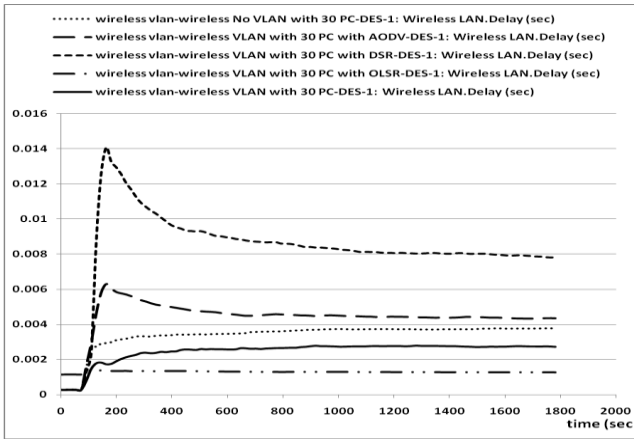


Figure 7. Delay for the case with and without VLAN scenarios employing 30 workstations.

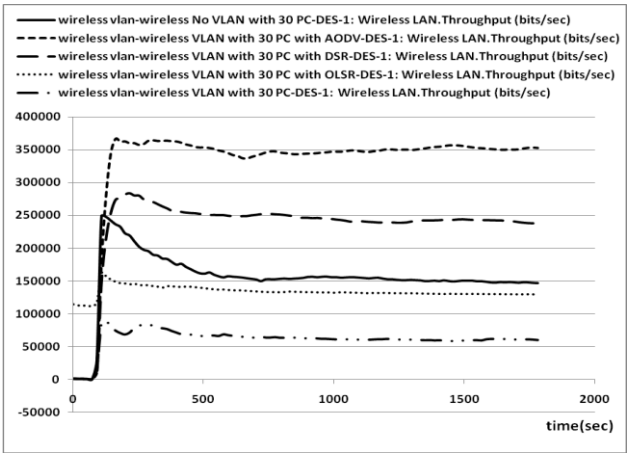


Figure 8. Throughput for the case with and without VLAN scenarios employing 30 workstations.

Finally, study to show the effect of traffic type on the performance of WLAN with and without VLAN together with routing algorithms have also conducted. In this investigation e-mail traffic and http traffic has been produced. All the scenarios investigated previously have tested with these two types of traffic. The results for the delay and throughput for such investigation gives the same conclusions as that shown in Figures 6-9.

VI. CONCLUSION

The study has introduced the usage Virtual LAN technology in securing wireless network. The study shows that such usage of VLAN will reduce the delay and throughput too. The reduction in throughput has been improved via the use of routing protocols such as AODV and OLSR.

The assessment also show that such improvement in VLAN and routing can also achieved as the number of workstation in the WLAN increased and for both type of popular traffic http and e-mail traffic. The results also show that the routing protocol type is an important factor to decide where delay can improved more or the throughput can be improved more. Therefore the study suggests the usage of intelligent system to decide which routing is used for the case of delay or the case of throughput requirement applications.

REFERENCES

[1] Y. B. ChoiG. Eason, J. Muller, C. V. Kopek and J. M. Makarsky, "Corporate wireless LAN security: threats and an effective security assessment framework for wireless information," Int. J. Mobile Communications, Vol. 4, No. 3, pp. 266-289, 2006.

[2] W. Huang and F. Kong , "The Research of VPN on WLAN" , International Conference on Computational and Information Sciences pp. 250 – 253, 2010.

[3] S. K. Sarkar , C Puttamadappa , and T. G Basavaraju "Ad Hoc Mobile Wireless Networks Principles, Protocols and Applications", Auerbach Publications, pp. 1-36, 2007.

[4] A. M. Al Naamany , A. Al Shidhani and H. Bourdoucen, "IEEE 802.11 Wireless LAN Security Overview", *IJCSNS International Journal of Computer Science and Network Security*, Vol.6 No.5B, pp. 138 – 156, May 2006.

[5] K. Okayama, N. Yamai, N. ; T. Miyashita, T. ; K. Kawano, K. ; T. Okamoto", A Method of Dynamic Interconnection of VLANs for Large Scale VLAN Environment", Proceedings. 6th Asia-Pacific Symposium on Information and Telecommunication Technologies, 2005. APSITT 2005.

[6] S. A. Jaro Alabady, "Design and Implementation of a Network Security Model using Static VLAN and AAA Server", *3rd International Conference on Information and Communication Technologies: From Theory to Application*, pp. 1-6, 2008.

[7] T. Wang and C. Yeh, "A Secure VLAN Construction Protocol in Wireless AD-HOC Networks", Information Technology: Research and Education. 3rd International Conference on **ISBN**: 0780389328, **pp.** 68-72**,** 2005.

[8] S. Y. Ameen and I. A. Ibrahimi, "MANET Routing Protocols Performance Evaluation with TCP Taho, Reno and New-Reno", International Journal of International Journal of uuuu---- and e an e and e---- Service, Science and Technology Service, Science and Technology Service, Science and Technology Vol. 4, No. 1, March 2011.

[9] G. Jayakumar and G. Gopinath, "Ad Hoc Mobile Wireless Networks Routing Protocols - A Review," *Journal of Computer Science*, Volume 3, Issue 8. 2007.