Journal of Applied Sciences

ISSN 1812-5654

science alert

ANSInet
an open access publisher
http://ansinet.com

Journal of Applied Sciences 9 (22): 3999-4005, 2009
ISSN 1812-5654

Enhancing Handoff Process using IAPP with Caching Techniques

Obay H. Sabrie and Rosli Salleh
Department of Computer Systems and Technology,
Faculty of Computer Science and Information Technology, University of Malaya,
Lembah Pantai, 50603 Kuala Lumpur, Malaysia

Abstract: This study propose a layer 2 method to enhance the handoff process through eliminating the scanning delay and reduce the time taken to perform a handoff by using Inter Access Point Protocol (IAPP) neighbor's discovery with access point and station caching techniques, in order to build a List of Neighbors and provide the station with the next possible AP to authenticate directly.

Key words: Handoff, wireless LAN, IEEE802.11, scanning delay

INTRODUCTION

One of the main problems in wireless networks is to support the mobility. When a Station (STA) moves around within a wireless network it goes out of the range of one access point (AP) and comes to the range of another one. The process of transferring the STA between these two APs are called a handoff process. This handoff process take about 400 msec and the scanning delay contributes almost 90% of it as proved by Mishra *et al*. (2003) and confirmed by Murray *et al*. (2007) that the scanning delay is an average of 275 m sec. This high delay will affect the real time and multimedia applications and cause service interruptions. The handoff process works in two different layers depending on the Network type if, the handoff performed between two APs inside the same network (Horizontal) then, the handoff process will use layer 2. On the other hand when, it performed between two access points in different networks (Vertical) the handoff will use layer 3 and a new IP should be assigned to the STA in order to communicate with the current network (Kim *et al*., 2008). This study proposes and implements a method to reduce the handoff delay for IEEE 802.11 WLAN layer 2 standard handoff process by eliminate the scanning delay. The method depends on providing the STA with a list of the next possible APs and their related information, in order for the STA to authenticate directly to the next AP without scanning. To build the List of Neighbors, the STA and AP will help each other in addition, to the IAPP that is used by the APs to communicate and exchange neighboring information.

The handoff process composing of three phases (IEEE Standard 802.11, 2007; LI *et al*., 2008) which are:

Discovery phase: The STA start to scan for another AP in its radio range with a better RSS (received signal strength) than the current AP. There are two scanning types defined by the IEEE 802.11 standard. Passive and active scanning, for passive scanning, the STA listen to the beacon messages broadcasted periodically by the APs depending on the maximum duration defined by the Max channel time parameter. The STA using passive scan must wait for the duration defined by the channel time parameter on each channel to collect all the beacon messages. After scanning all channels the beacons will be processed and the best AP will be selected. For active scanning the STA broadcasts a probe request in each channel to scan and wait for a probe response from all reachable APs. The STA waits a period of time for the probe responses called minimum channel time if no response or traffic detected then, the channel assumed to be empty and the STA switches to the next channel. However, if a probe response detected then, the STA assumes that at least one AP may exist and wait on that channel until the maximum channel time expires to give time for other APs responses to be received (Gast, 2005). In active scan two types can be used, the full scan and during this one the STA scans all the channels available and the short or selective scan that reduce the number of scanned channels because the STA scans only the channels that do not overlap. In the IEEE 802.11b/g standard using 2.4 GHz spectrum there are 11 channels only 3 channels do not over lap (1, 6 and 11), for IEEE 802.11a using 5 GHz spectrum there are 8 channels that do

Corresponding Author: Obay H. Sabrie, Department of Computer Systems and Technology,
Faculty of Computer Science and Information Technology, University of Malaya, Lembah Pantai,
50603 Kuala Lumpur, Malaysia

not overlap (Walke *et al*., 2006). A third type of scanning may considered which is scanning with neighborhood detection (Pries and Heck, 2004), during this type the STA should know the MAC address and current channel of the AP to be scanned first, that reduces the time spend in scanning all the APs available.

Re-authentication phase: This phase transfers the STA identity from the old AP to the new AP, which is the best AP found in the first phase. The STA send a re-authentication request and wait for a re-authentication response from the AP to approve or reject the authentication. The IEEE 802.11 standard defines two sub types of authentication, first is the open system authentication which is a null authentication algorithm. Any STA request for authentication may authenticate if the AP configuration set to open system authentication. Second is the shared key authentication that depends on a shared secret key and authenticate only the STA who knows that key (IEEE Standard 802.11, 2007), other wise the AP reject the authentication. Shared secret key delivered to the selected members via a secure channel that is independent from the IEEE 802.11, the WEP must be selected in both sides in order to use the shared key authentication method.

Re-association phase: In this phase the STA send a re-association request and wait for the response from the AP. Before the re-association phase complete the STA is receiving data from the old AP. But after the re-association complete the STA receive the data from the new AP and disassociate from the old AP. By the end of this phase the handoff process complete.

MATERIALS AND METHODS

The IAPP defined in the IEEE 802.11f standard (IEEE Standard 802.11F, 2003) to be used to transfer context information between APs and reduce association delay.

This method uses the IAPP to exchange neighboring information between APs. The method considers two sides, the STA side and the AP side.

STA side operations: The STA enters the wireless network coverage area and receive a beacon frame send regularly by the AP. The handoff method add another two fields to the original beacon frame defined by IEEE 802.11 standard, the first one is the AP Neighbors List field that contains a list of available neighboring APs and their information such as BSSID (MAC address), SSID, channel number and other related information needed during handoff process. Figure 1 shows the modified beacon frame.

The second field is the SL field, this field is used to indicate if the AP Neighbors List inside the received beacon is empty or not in order to reduce the time taken during processing a beacon frame with an empty AP Neighbors List by the STA. Whenever the STA receives a beacon frame, it will check the SL field value. If the field value equals to one, that means the AP Neighbors List is not empty and the STA must update its Scan Lock value to one, in order not to start a full active scanning when a handoff needed. The STA then, opens the AP beacon frame and copy the AP Neighbors List information into the STA Caching List. After storing list information, the STA continues to communicate with the current AP until the RSS goes under a specific threshold TH value. This TH is used to trigger the handoff process. When the handoff process starts and the Scan Lock value equal to one, the STA skip the full active scanning process and starts the authentication process directly with the first AP in the STA Caching List. The authentication process is done by sending authentication request frame by the STA and waiting for authentication response. In case the authentication fails, the STA resend the authentication request frame for a second time to give another chance for the AP to respond and to make sure that the AP is not available. If there was no response after two transmissions, the STA will try to authenticate with the second AP in the STA Caching List and so on until the STA will be authenticated and connected. On the other hand, if the STA Caching List end was reached without authenticating the STA then the STA will start a full active scanning. Figure 2 shows the STA side operations flow chart.

The other case that the STA needs to perform a full active scanning is when the SL field value is equal to zero, in this case the STA discard the AP Neighbors List contents in the beacon frame and update the Scan Lock value to zero then, start a full active scanning. The STA performs a full active scanning by sending a probe request on each channel and wait for a probe response from APs in range. The probe response frame contains AP information such as BSSID (MAC address), SSID, channel number and other related information. When the STA receives the response frame, it will store the information in the STA BSS List then, sort the APs according to the RSS. After receiving the probe response frame from all the APs in range, the STA will authenticate with the best AP

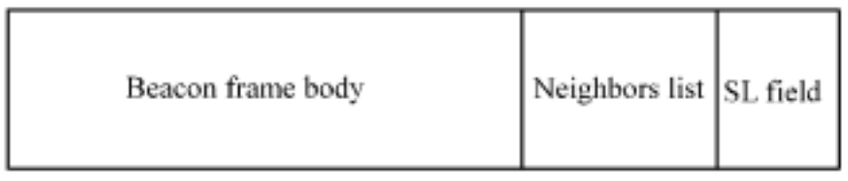

Fig. 1: Modified beacon frame

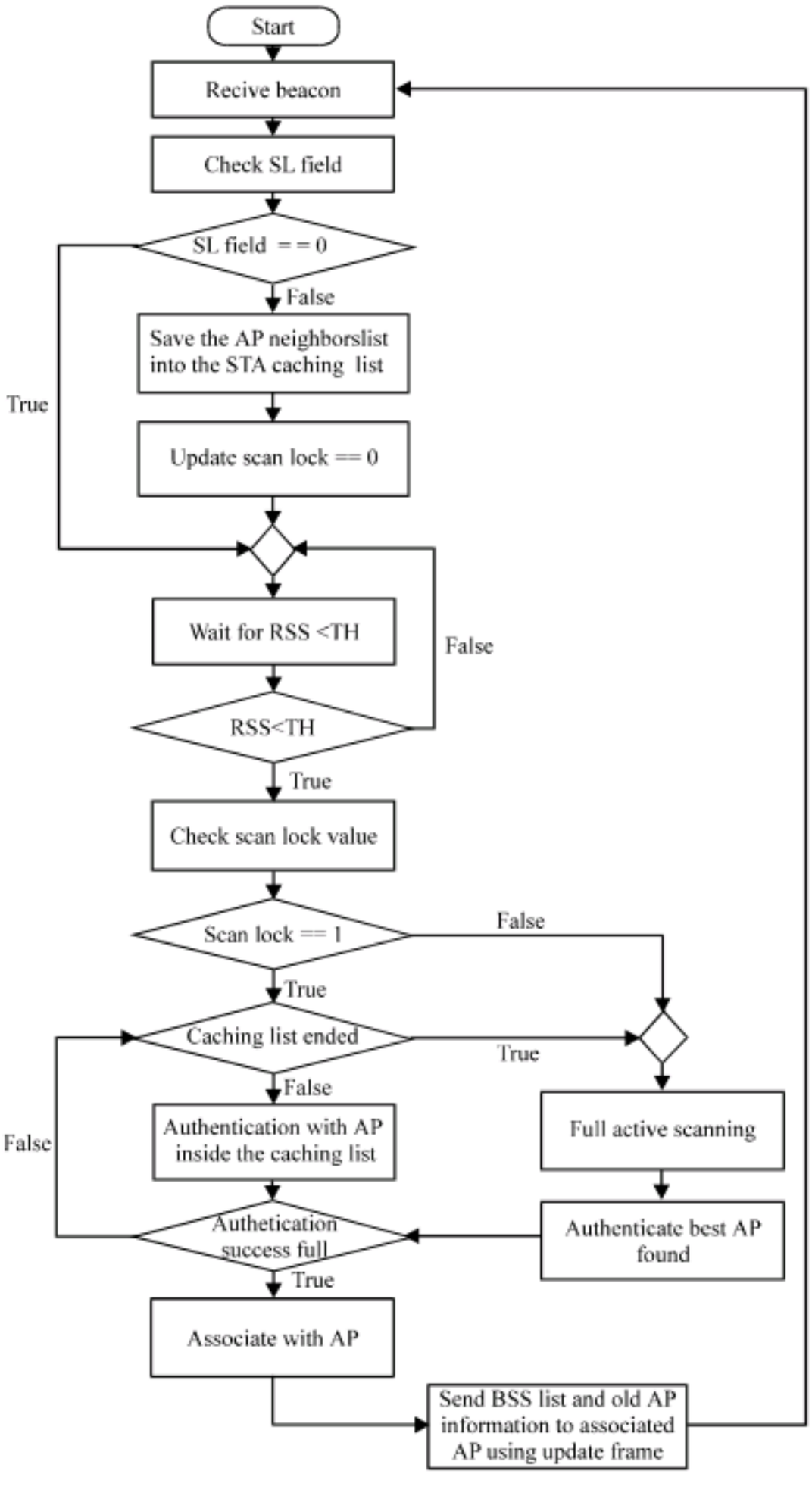

Fig. 2: STA side operations flow chart

founded and sends the STA BSS List that contains the APs founded during the full active scanning and the old AP information to the currently associated AP. The STA sends this list inside a new IEEE 802.11 management frame called the Update Frame.

AP side operations: The STA will send the STA BSS List to the current AP where the STA is associated using the update frame, the AP will open the frame and start comparing and saving the information into the AP Neighbors List. The received information can be a BSSID (MAC address), SSID, channel number and other related information collected by the STA during the full active scanning. If the STA BSS list neighboring AP information already exists inside the AP Neighbors List, no update will be made and the checking continues with the next AP in the STA BSS list. However, if the AP information is not existed inside the AP Neighbors List then, the AP information will be copied to the AP Neighbors list and to the AP update list. This process will continue until the STA BSS list ends. When the aving process is completed, the AP update list

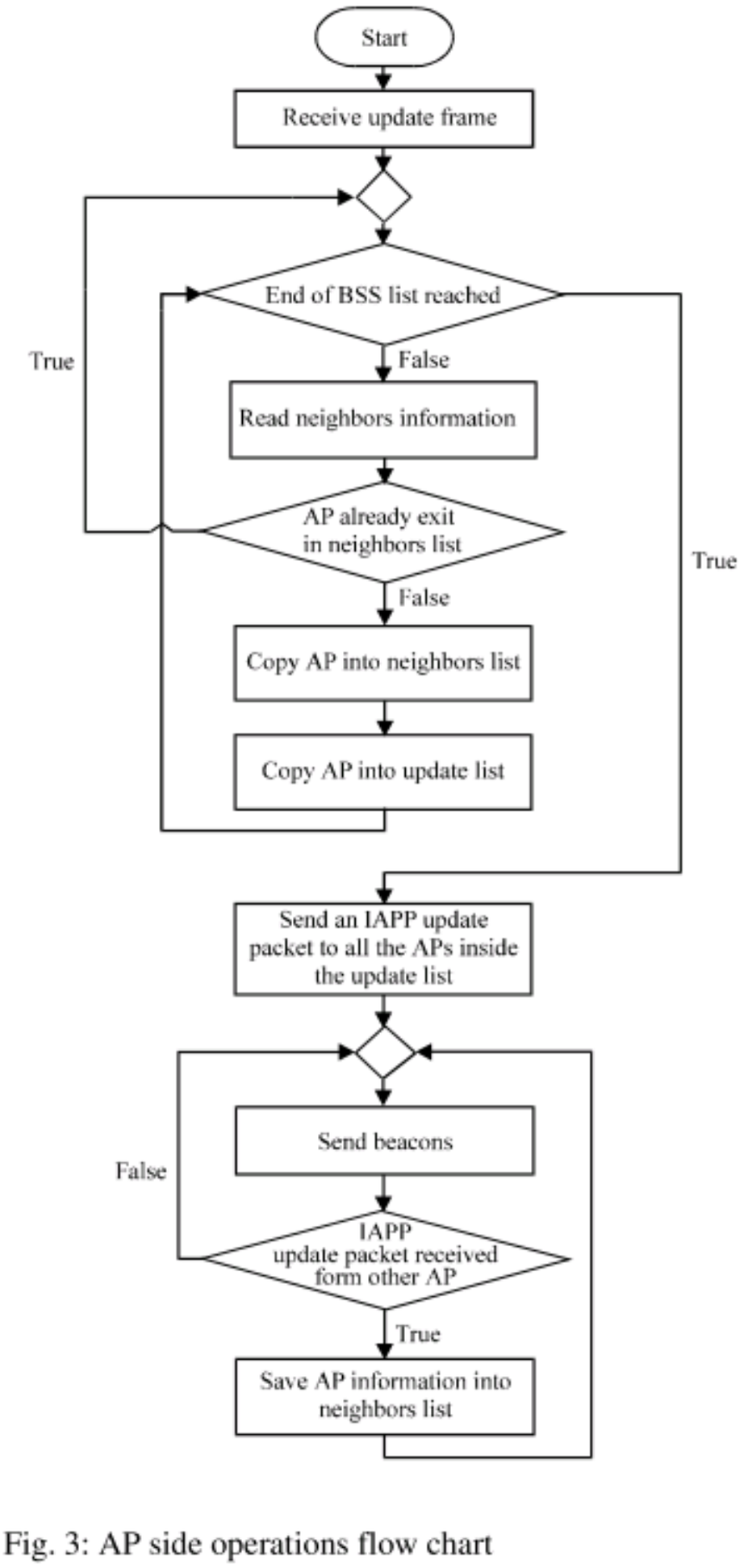

Fig. 3: AP side operations flow chart

will contain only the new discovered neighboring APs information. However, the AP Neighbors List contains all the neighboring APs information (including old information from previous updates). The AP update list will be used by the current AP in order to contact the APs inside this list using IAPP. The current AP will send a new IAPP update packet that contains its BSSID (MAC address), SSID, channel number information to the neighboring APs exist in the AP update list. This IAPP update packet is used to inform them that the current AP is already a neighbor.

The AP update list is used instead of the AP Neighbors List during update in order to reduce the impact on the network as only the new APs found will be updated with the current AP information. However, if the AP sends IAPP update packet to all the APs based on the AP Neighbors List, there may be APs that have been already updated from previously sent packets. Consequently, this impacts extra time and load on the AP. When the neighboring AP receives an IAPP update packet, it will check its AP Neighbors List for the existence of this information. If the AP information that is sent is not found then, it will update its AP Neighbors List information. Otherwise if the neighbor already exists in the AP Neighbors List then, the AP will discard the IAPP Update Packet. Finally, after the AP Neighbors List is updated, the AP set the SL field value to one and starts sending this AP Neighbors List inside the beacon frames. Figure 3 shows the AP side operations flow chart.

RESULTS

The method was implemented using the OMNeT++ simulator with INET Framework in top. Then, the results of the implemented method were compared to the IEEE 802.11 standard handoff results to explain the benefits of using the new method fast handoff over the existing standard.

Handoff delay: The handoff delay for the STA moving from one AP to another was calculated during the simulation time and three delays were found. The first delay represents the IEEE 802.11 standard handoff that use the full active scan during the discovery phase and the handoff delay was about 414 m sec. the second delay represents the implemented method that eliminates the scanning delay and authenticate directly to the first AP inside the STA Caching List. The handoff delay was almost 2 m sec. The third delay represents the implemented method that eliminates the scanning delay and authenticates directly to the last AP inside the STA Caching List (when the best AP is the last AP in the list). As the STA try to authenticate two times with each AP to make sure its not responding before moving down to the next AP in the list so, the handoff delay was 4 m sec. Figure 4 shows the handoff delay times.

Ping packet lost: The STA sent ping request to the server 3 times each, with 2889 packets within 13 sec simulator time period and size of 56 bytes. The first group of packets was sent during a handoff process using an IEEE 802.11 full active scanning. The STA received 2752 packets which mean that, the number of lost packets was 137.

The second group of packets was sent during the handoff process using the fast handoff method. The STA

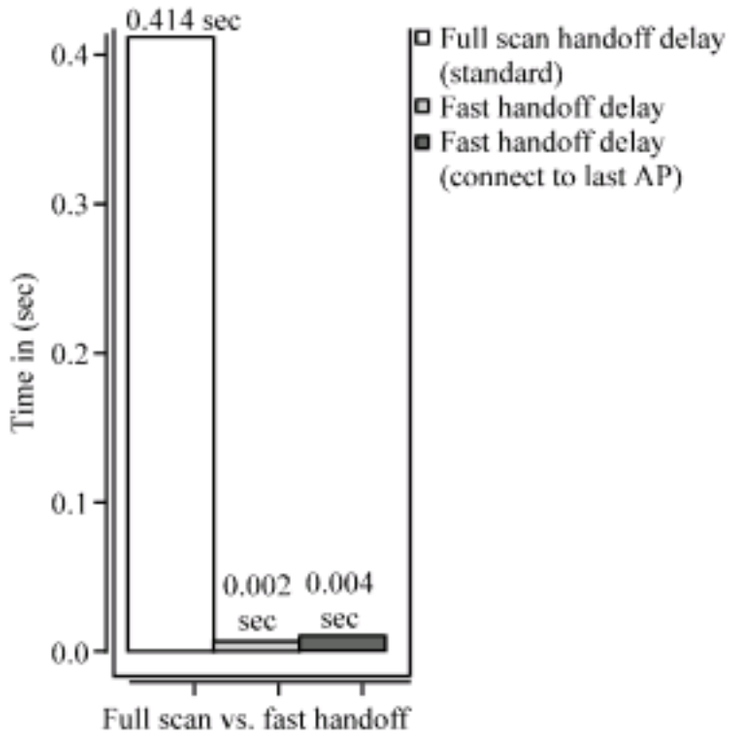

Fig. 4: Handoff delay times chart

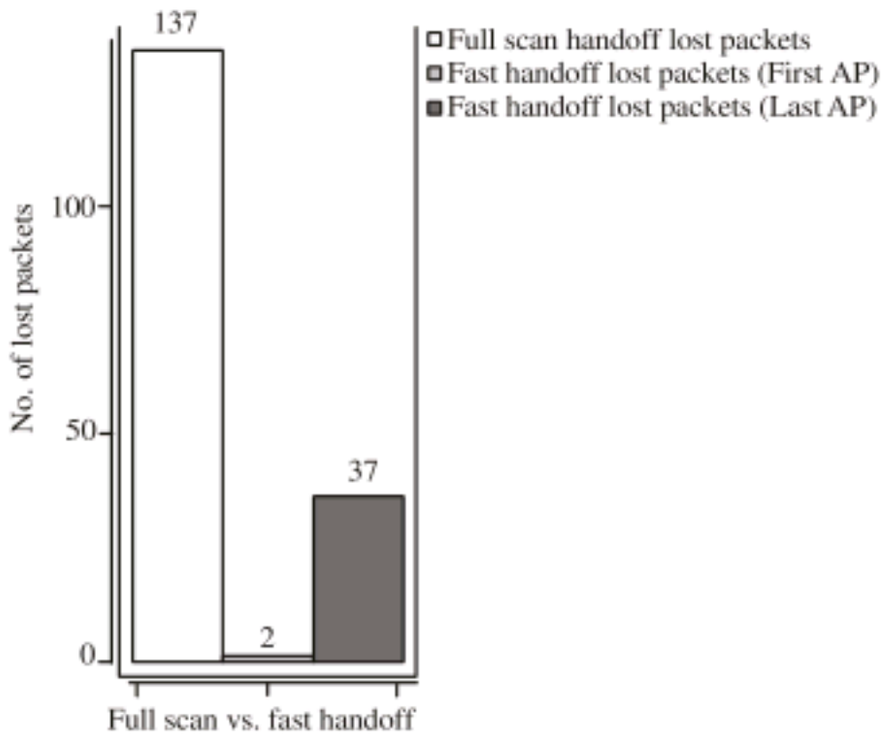

Fig. 5: Number of lost packets chart

authenticate directly to the first AP in the STA Caching List and during the handoff the STA sent 2889 packets and receive 2887 packets which mean that, the number of lost packets was 2.

The third group of packets was sent during the handoff process using the provided method. The STA try to authenticate directly with all the APs inside the STA Caching List then, successfully authenticate with the last AP inside the list. During the handoff the STA send 2889 packets and receive 2852 packets which means the number of lost packets is 37. Figure 5 shows the number of lost packets for each case.

The implemented handoff method provides a significant enhancement to the handoff process comparing with the IEEE80.11 standard by eliminating the scanning delay and as a result reducing the total handoff delay from 414 m sec in the standard to 2 m sec using the method.

The method used need to exchange information between the APs using IAPP update packet in order to exchange the neighboring information and build the AP Neighbors List. This IAPP messages does not have a high impact on the network as its used only during building the Neighbors Lists and when there is a change in the topology. In addition, using a full duplex Ethernet connection reduce any serious effects on the network.

The neighboring information send from the AP to the STA is added to the original beacon frames that send regularly by the AP so, no extra effect is appeared.

DISCUSSION

The scanning delay within the discovery phase cause almost 90% of the total handoff delay as proved practically by Mishra *et al*. (2003). It was clear that the wireless hardware type affect the handoff delay. In addition different configurations may affect the delay time such as the Min channel time and Max channel time values. Our method was able to eliminate the scanning delay and enhance the handoff process by 98% over the IEEE 802.11 standard handoff process by providing the STA with a list of its possible neighbors to authenticate directly and this is different from the standard handoff when the STA should scan each channel searching for APs in range, this operation cause the STA to search channels even if it's empty (IEEE Standard 802.11, 2007). To reduce the number of channels scanned a selective scan was provided to scan only the channels that do not overlap, for example in IEEE 802.11b 2.4 GHz 8 channels available only 3 do not overlap so the selective scan search these channels and discard the others as provided by Sangho *et al*. (2004). However, the selective scan is not very effective when it used with 802.11a because there are 8 channels do not overlap and need to be scanned. Most of the researches that use the selective scan combine it with other techniques to provide better results. Further more the scanning delay can be reduced if the STA knows which AP to probe directly without scanning using the NG neighbor graphs to provide the locations of the APs in the network making it easier for the STA to find the best near by AP to connect. As explained by Minho *et al*. (2004) the handoff can be reduced if the STA knows the surrounding APs locations. They provide two algorithms to reduce the handoff latency. The first one is the NG neighbor graph algorithm that aimed to reduce the number of channels to be probed probe-channel count by knowing the locations and channels used by neighboring APs. The STA probe only these APs channels to reduce the probe count. In the other hand, to reduce the waiting time for a probe response on

each channel probe-wait time, the STA moves to probe the next channel when no more APs expected to respond on the current one. The second algorithm called NG pruning algorithm and it depends on the knowledge of non-overlap APs in order for the STA to prune all APs that did not overlap with current reachable AP and this can reduce the number of channels to be scanned. The APs defined to be non-overlap when the STA can not communicate with both APs using acceptable signal strength at the same time. The NG can be provided by a server as used by Kim *et al*. (2004). They use a neighbor graph NG server that stores the APs topology and provide the STA with the AP neighbors along with the number of channels used to allow the STA scans only the channels used by the APs. The less number of channels scanned provides less handoff delay. However, because a centralized server stores a static NG files any server failure or topology changes without updating the NG server may cause a failure and push the STA to use a standard scanning methods causing more handoff delay. Chintala and Qing-An (2007) used the IAPP to reduce the scanning delay by providing an extended probe message with the MAC address of the current AP included, to allow other near by APs to reply the probe response to the current AP and not directly to the STA, in order to reduce the waiting time of the STA on each channel. This method reduce the scanning delay but the STA still have to scan all the channels even if it is not waiting for the probe response to be received. Direct authentication with fast scan to find AP used by Zhang and Pierre (2008). They provided a fast scanning method starts in the STA when the pre-defined trigger value goes under specific threshold. The STA start scanning for neighboring APs and once the first AP sends a response then, the STA starts the authentication phase directly by sending authentication request and wait for authentication response from the AP to connect. This method reduces the time taken to scan all channels by connecting directly to the first acceptable AP but that does not means that it is the best AP in range and in some cases the AP located at the last scanned channel, what makes the handoff delay high.

CONCLUSIONS

This study provides a layer 2 handoff method for the IEEE 802.11 wireless LAN. The method was able to eliminate the scanning delay and enhance the total handoff process by using the IAPP to exchange the neighboring information between the APs, after the AP receives this information from the STA after the full scan process. The AP sends the composed Neighbors List to the STA.

Using the modified beacon frame and when a handoff is needed the STA use the Neighbors List to authenticate directly to the first AP inside the list. This method reduces the handoff delay to be 2 m sec comparing to 414 m sec using the IEEE 802.11 standard. In addition, this method provides dynamic distributed neighbors caching that provide updated information for the current status of the network and guarantee a high cache hit.

REFERENCES

Chintala, V.M. and Z. Qing-An, 2007. Novel MAC layer handoff schemes for IEEE 802.11 wireless LANs. Proceedings of the IEEE Wireless Communications and Networking Conference, Mar. 11-15, Kowloon, pp: 4435-4440.

Gast, M.S., 2005. 802.11 Wireless Networks: The Definitive Guide. 2nd Edn., O'Reilly Media Inc., USA., ISBN: 978-0-596-10052-0.

IEEE Standard 802.11, 2007. IEEE Standard for Information Technology Telecommunications and Information Exchange Between Systems Local and Metropolitan Area Networks Specific Requirements, Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications. Institute of Electrical and Electronics Engineers, New York, USA.

IEEE Standard 802.11F, 2003. IEEE Trial-Use Recommended Practice for Multi-Vendor Access Point Interoperability via an Inter-Access Point Protocol Across Distribution Systems Supporting IEEE 802.1 Operation. Institute of Electrical and Electronics Engineer, New York, USA.

Kim, H.S., S.H. Park, C.S. Park, J.W. Kim and S.J. Ko, 2004. Selective Channel Scanning for Fast Handoff in Wireless LAN Using Neighbor Graph. In: Personal Wireless Communications, Niemegeers, A. and S.H. de Groot (Eds). LNCS 3260, Springer Verlag, Berlin Heidelberg, ISBN-13: 978-3-540-23162-2, pp: 194-203.

Kim, D.H., W.T. Kim, H.G. Lee, S.J. Kim and C.H. Lee, 2008. A performance evaluation of vertical hanover architecture with low latency handover. Proceedings of the International Conference on Convergence and Hybrid Information Technology, Aug. 28-30, IEEE Computer Society, Washington, DC. USA., pp: 66-69.

LI, C.S., Y.C. Tseng, H.C. Chao and Y.M. Huang, 2008. A neighbor caching mechanism for handoff in IEEE 802.11 wireless networks. Springer Science Business Media, LLC 2008.

Minho, S., M. Arunesh and A.A. William, 2004. Improving the latency of 802.11 hand-offs using neighbor graphs. Proceedings of the 2nd International Conference on Mobile Systems, Applications and Services, Jun. 6-9, ACM, New York, USA., pp: 70-83.

Mishra, A., M Shin and W. Arbaugh, 2003. An Empirical Analysis of the IEEE 802.11 MAC Layer Handoff Process. ACM, USA.

Murray, D., M. Dixon and T. Koziniec, 2007. Scanning delays in 802.11 networks. Proceedings of the International Conference on Next Generation Mobile Applications, Services and Technologies, Sept. 12-14, IEEE Computer Society, Washington, DC. USA., pp: 255-260.

Pries, R. and K. Heck, 2004. Performance comparison of handover mechanisms in wireless lan networks. Institute of Computer Science, Research Report Series No. 339. http://www.emmelmann.org/Library/Papers_Reports/docs/tr339.pdf.

Sangho, S., G.F. Andrea, A.S. Rawat and G.S. Henning, 2004. Reducing MAC layer handoff latency in IEEE 802.11 wireless LANs. Proceedings of the 2nd International Workshop on Mobility Management and Wireless Access Protocols. Oct. 1, ACM, New York, USA., pp: 19-26.

Walke, B.H., S. Mangold and L. Berlemann, 2006. IEEE 802 Wireless Systems (Protocols, Multi-hop Mesh/Relaying, Performance and Spectrum Coexistence). John Wiley and Sons Ltd., England, ISBN-13: 978-0-470-01439-4.

Zhang, L.J. and S. Pierre, 2008. Optimizing the performance of handoff management in wireless LANs. Int. J. Comput. Sci. Network Sec., 8: 87-94.