A Redundant Neighborhood Approach to Tolerate Access Point Failure in IEEE 802.11 WLAN

Manmath Narayan Sahoo[1], Pabitra Mohan Khilar[2], Banshidhar Majhi[3]
[123]Department of CSE, NIT Rourkela,
Orissa-769008, India
{[1]sahoom, [2]pmkhilar, [3]bmajhi}@nitrkl.ac.in

Archived in Dspace@nitr

A Redundant Neighborhood Approach to Tolerate Access Point Failure in IEEE 802.11 WLAN

Manmath Narayan Sahoo[1], Pabitra Mohan Khilar[2], Banshidhar Majhi[3]
[123]Department of CSE, NIT Rourkela,
Orissa-769008, India
{[1]sahoom, [2]pmkhilar, [3]bmajhi}@nitrkl.ac.in

***Abstract*— Because of failure of an access point In IEEE 802.11 WLAN, some or all the mobile stations connected to the network via that access-point may lose connectivity. In this paper, the problem of enhancing the survivability of IEEE 802.11 WLAN focusing on tolerating Access Point (AP) failures is addressed. In particular, focus on the problem of overcoming these APs failure working with reconfiguration of the remaining APs by changing parameters like the neighboring AP's MAC address is done. This approach consists of two main phases: Design Phase and Fault Response. In Design phase, we deal with quantifying, placement and setting up of APs according to both area coverage and performance criteria. In Fault Response phase we consider the reconfiguration of the active APs in order to deal with AP failure in the service area.**

***Keywords*— Access Points, Wireless Distributed System, Basic Service Set, Extended Service Set, Wireless LAN**

I. INTRODUCTION

Wireless networks have been growing rapidly in the past years to support increasing demands for mobile communications. Therefore since last few years it has been a vast area of research.

In IEEE 802.11 terminology a "Distribution System" [8] is a system that interconnects so-called Basic Service Sets (BSS). A BSS is best compared to a "cell", driven by a single Access Point. Wireless Distribution System is normally used in large, open areas where pulling wires is cost prohibitive, restricted or physically impossible [3]. Critical applications, such as stock trading, health monitoring systems etc., require the underlying network to continue to function even in the presence of faults [1]. Unfortunately, current wireless networks are notoriously prone to a number of problems, such as the loss of link-level connectivity due to user mobility and/or infrastructural failures, which makes it difficult to guarantee their reliability.

For wireless (and wire-line) networks, a network's ability to avoid or cope with failure is measured in three ways [2]: *Reliability* is a network's ability to perform a designated set of functions under certain conditions for specified operational times. *Availability* is a network's ability to perform its functions at any given instant under certain conditions. Average availability is a function of how often something fails and how long it takes to recover from a failure. *Survivability* is a network's ability to perform its designated set of functions given network infrastructure component failures, resulting in a service outage, which can be described by the number of services affected, the number of subscribers affected, and the duration of the outage.

Our research addresses the issues surrounding the reliability and survivability of wireless local area networks. In this paper, we propose a cost-effective mechanism to improve fault tolerance during access point failures in IEEE 802.11 WLAN.

The reminder of the paper is organized as follows: section II presents the architecture of WLAN and describes different components of it. Section III outlines the related works that are already in place in this area. In section IV we present our proposed algorithm along with a worked out example. Section V discusses the simulation results and finally section VI concludes our research work and gives future research directions.

II. ARCHITECTURE OF WIRELESS LAN

Various components of Wireless LAN are depicted in figure 1 and are described below.

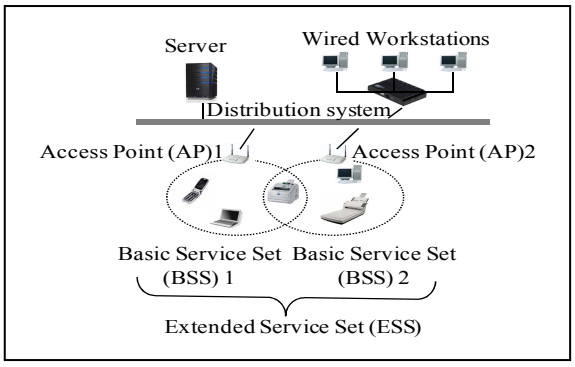

Fig. 1 Wireless LAN Architecture

A. Stations

All components that can connect into a wireless medium in a network are referred to as stations. All stations are equipped with wireless network interface cards (WNICs).

B. Basic Service Set

The Basic Service Set (BSS) is a set of all stations that can communicate with each other. There are two types of BSS **[9]**: Independent BSS (also referred to as IBSS) and Infrastructure BSS. Every BSS has an id called BSSID; it is the MAC address of the Access Point servicing the BSS. An *Independent BSS* is an ad-hoc network that contains no Access Points. Since they do not use Access Points they can't connect to any other basic service set. An *Infrastructure BSS* can communicate with

978-1-4244-4837-1/09/$25.00 ©2009 IEEE

other stations not in the same basic service set by communicating to each other through Access Points.

C. Extended Service Set

An Extended Service Set (ESS) is a set of connected BSS. Access Points in an extended service set are connected by a distribution system.

D. Distribution System

A Distribution system connects Access Points in an extended service set. A distribution system is usually a wired LAN but also can be a wireless LAN.

E. Wireless Distribution System

When it is difficult to connect all of the Access Points in a network by wires, wireless interconnection of access points in an IEEE 802.11 network is required and in that case the distribution system is called as a *Wireless Distributed System* **[9]**. It allows a wireless network to be expanded using multiple access points without the need for a wired backbone to link them, as is traditionally required

III. Related Work

A redundancy technique has been described by Rajeev Gandhi [5] to tolerate access-point failures in wireless networks in which, additional access-points are designated as a backup, and are activated once the primary (the previously operational) access-point fails. In this technique, the backup access-point must be able to detect the primary access-point's failure; also, as a part of fault recovery, all the mobile stations that were associated with the failed access-point must switch over to the backup access-point. Apart from the inherent latency involved in detecting access-point failures and performing the fail-over, this results in additional infrastructure costs. Rajeev Gandhi [5] describes another technique called *overlapping coverage approach* to tolerate access point failure in wireless network. The principal idea in providing overlapping coverage across different access points is that, if one access-point fails, mobile stations associated with that access-point can be transferred over to another access-point whose coverage area intersects with that of the failed access-point.

Snow et al. [2] describe the use of multifunction/multimode devices to tolerate access point failure in wireless network, in which a single terminal offers multiple interfaces. Thus a single terminal can be connected to a wireless LAN, satellite, cordless access and a cellular network with different interfaces. If any of the networks fails the terminal remains connected via other links. Snow et al. [2] describe the use of overlay network to improve survivability and hide access point failure.

Hass et al. [6] describe a technique to tolerate the failure of the location database, which is a repository of the locations of mobile stations at the mobile switching centers in PCS network. Chen et al. [11] describe a scheme for enhancing the connection reliability in WLANs by tolerating the existence of *shadow regions* through placement of redundant APs. But the presence of redundant APs, may lead to *co-channel interference* problems. But our scheme is not based on redundancy and does not require shadow APs. Tipper et al. [4],[7] present a survivability analysis of Personal Communication Service (PCS) networks. The results of their simulation model demonstrate that user mobility can significantly degrade the performance of the network, in the presence of failures.

IV. Proposed Algorithm

A simple fault detection approach, based on response timeout, which promises to be more cost-effective to identify failures, is developed. In particular, focus on the problem of overcoming these APs failures working with reconfiguration of the remaining APs by changing parameters like the neighboring AP's MAC address is done. This approach consists of two main phases: *Design* and *Fault Response*. In Design phase, we deal with quantifying, placement and setting up of APs according to both area coverage and performance criteria. In Fault Response phase we consider the reconfiguration of the active APs in order to deal with AP fault in the service area.

A. Design Phase (Algorithm for Establishing Route)

Statement: This algorithm finds the minimum spanning tree and assigns redundant MAC IDs to each node of the minimum spanning tree for network survival in case of AP failure.

Input:

1. Location of access points (Latitude and Longitude),
2. Range of the access points.

Output:

1. MAC ID for establishing the network.
2. Redundant MAC ID for network survivability.

The algorithm consists of 6 main steps which are described in figure 2.

B. Fault Response Phase (Network Survivability Algorithm)

Statement: This algorithm is used to make the network survive in case of failure of any node (AP).

Input:

1. The modified weight adjacency matrix of the network,
2. The MAC ID list associated with each node,
3. The minimum spanning tree generated by above algorithm.

Output:

1. A connected network consisting of the remaining active APs.

The algorithm consists of 3 main steps which are described in figure 3.

Step 1: For 'n' nodes construct adjacency matrix A[n][n], where A[i[][j] represents the distance between the node i and j (Distance is calculated from latitude and longitude).Enter the threshold value 'T'.

Step 2: Update the adjacency matrix by comparing each element A[i][j].

If A[i][j] > T then, make A[i][j]=0,

as the nodes are not valid for being out of WiFi range.

Step 3: Find the minimum spanning tree from the matrix A[n][n].

Step 4: Apply BFS to the graph and store the traversing sequence in an array BFS[ ].

Step 5: Store adjacent node's MAC ID in each node of the spanning tree.

- Each spanning tree node has an array Neighbor[ ] associated with it.
- This array is used to store the MAC ID of the adjacent nodes in minimum spanning tree.

Step 6: Find valid redundant nodes for each node in BFS [ ] and insert valid MAC IDs.

```
For i=n-1 to 0 continue
   For j=i-1 to 0 continue
      If ( BFS[j] is valid node for BFS[i] ) then
         Insert MAC ID of BFS[j] to the MAC ID
         array of BFS[i] only when the MAC ID is not
         previously present.
      End if
   End for
End for
```

Fig. 2 Algorithm for establishing route

Step 1: Apply DFS to the spanning tree and store the traversing sequence in an array DFS[ ].

Step 2: Find failure node (say F) applying ping between starting node and the node in DFS[ ].

Step 3:

For each adjacent node N of F in the spanning tree continue

Find the adjacency list L of node N from the modified weight adjacency matrix.

For each node in L continue

Store the MAC ID in N's Neighbor[ ] iff it is not already present and does not form a loop.

End for

End for

Fig. 3 Network Survivability Algorithm

C. An illustrated Example

Algorithm for Establishing Route

Step 1: The complete graph for 7 APs is shown in Figure 4 along with the initial weight adjacency matrix in Table I.

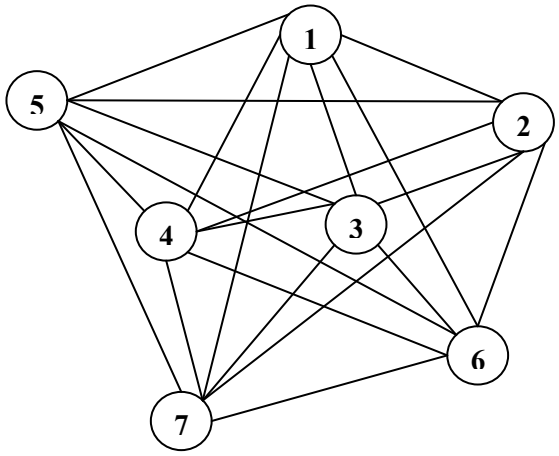

Fig. 4 Complete graph for Access Point network

TABLE I
INITIAL WEIGHT ADJACENCY MATRIX

	1	2	3	4	5	6	7
1	0	4	8	9	5	12	11
2	4	0	5	8	7	7	9
3	8	5	0	5	11	5	8
4	9	8	5	0	5	12	6
5	5	7	11	5	0	13	11
6	12	7	5	12	13	0	7
7	11	9	6	8	11	7	0

Step 2: Checking the threshold value, T=9, the adjacency matrix is modified (shown in Table II) and the modified graph is found as shown in Figure 5

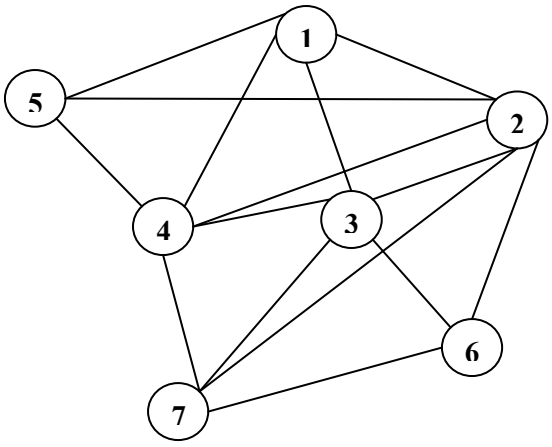

Fig. 5 Modified graph for Access Point network

TABLE II
MODIFIED WEIGHT ADJACENCY MATRIX

	1	2	3	4	5	6	7
1	0	4	8	9	5	0	0
2	4	0	5	8	7	7	9
3	8	5	0	5	0	5	8
4	9	8	5	0	5	0	6
5	5	7	0	5	0	0	0
6	0	7	5	0	0	0	7
7	0	9	6	8	0	7	0

Step 3: Minimum spanning tree of the modified graph is depicted in Figure 6.

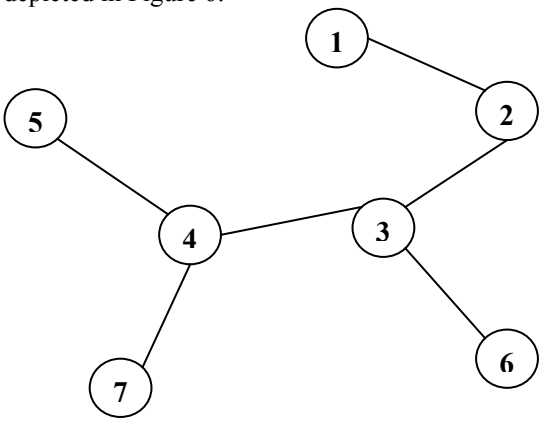

Fig. 6 Minimum spanning tree of the modified graph

Step 4: The BFS traversal sequence of the modified graph is 1,2,5,3,4,6,7

Step 5: Figure 7 shows the initial neighborhood MAC ID assignments

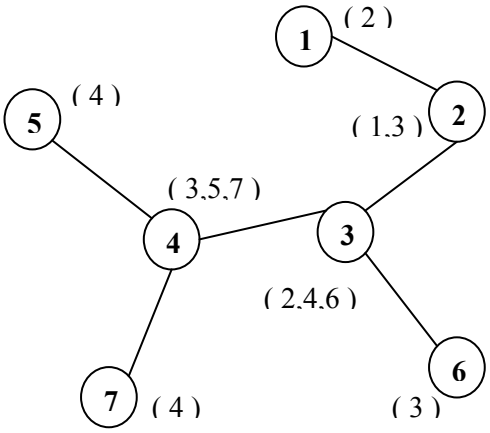

Fig. 7 Access points with neighbor MAC IDs.

Step 6: Figure 8 shows redundant MAC ID assignments to the minimum spanning tree.

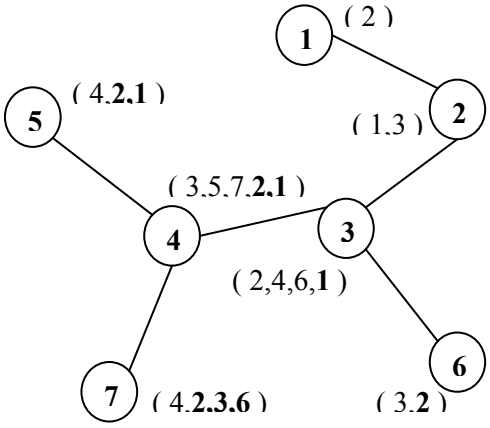

Fig. 8 Access Points with neighbor and redundant MAC Ids

Network Survivability Algorithm

Step 1: Output of DFS traversal sequence of the minimum spanning tree is 1,2,3,4,5,7,6

Step 2: Ping to the access points in the DFS sequence.
Ping to AP 1: It is responding.
Ping to AP2: It is not responding.
Again ping to AP 1: It is responding.
This implies AP 2 has failed.
i.e. F=2

Step 3: The neighboring nodes of F (=2) are 1 and 3.

By placing AP3 as the neighbor of AP1 all the active APs become connected and it does not lead to loop formation. Figure 9 shows the final network after survival.

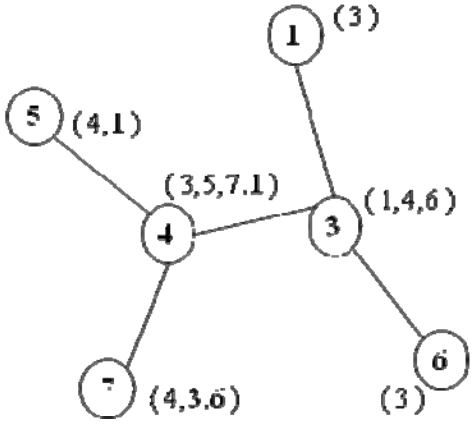

Fig. 9 Final Network after Survival

V. SIMULATION AND RESULTS

In this section we present the results of our simulations, which we performed in *ns-2* to evaluate the efficiency of our algorithm. We tested our algorithm on a 3.0GHz processor, in Linux (Ubuntu 8.04) environment and below we report the result of one such simulation scenario. To get each point in the graph we considered the average no of clock cycles for 10 executions of our algorithm for networks or different size and

we have compared the result of this algorithm with the algorithm proposed in [10] as shown in figure 10.

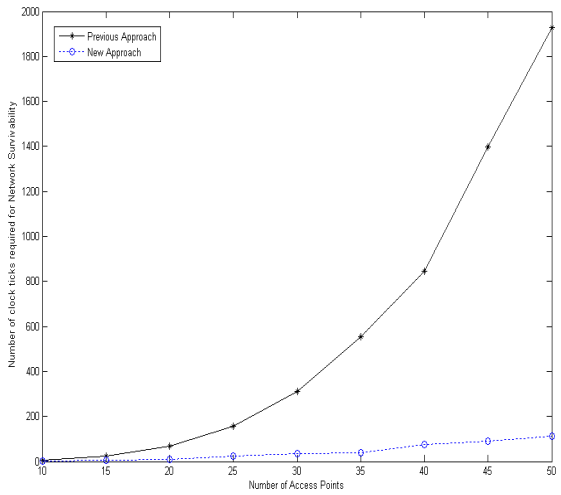

Fig. 10 Variation of no of clock cycles required for network survivability w.r.t Network size

The graph depicts how the no of required clock cycles to maintain network connectivity in case of AP failure varies with respect to the change in network size i.e. with respect to the change in no of access points in wireless LAN. The behaviour of the graph implies that, as the network size increases with respect to the no of access points, no of clock cycles required to maintain network connectivity in case of access point failure also increases. The behaviour is obvious because with the increase in no of APs, the size of the neighborhood list of a failed AP also increases thus step 3 of network survivability algorithm takes more no of clock cycles to complete its execution. So the no of clock cycles required not only depends on the no of APs but also on the network structure. It is also clear from the graph that the new approach takes a linear increment over the no of clock cycles required where as the previous approach requires an exponential increment. Hence we can substantiate that the performance of the new approach is better than the previous one.

VI. CONCLUSIONS

In this paper, we have proposed a survivability scheme for IEEE 802.11 Wireless Local Area Network in case of AP failure. This algorithm can be used to make the network survive dynamically with the assumption that each Access Point must have place to hold the redundant MAC IDs of neighboring APs. A simple fault detection approach, based on response timeout, which promises to be more cost-effective to identify failures due to lack of energy to an AP or problems with the wired link to an AP is developed. In particular, focus on the problem of overcoming these APs failures working with reconfiguration of the remaining APs by changing parameters like the neighboring AP's MAC address is done. This approach consists of two main phases: Design and Fault Response. In Design phase, we deal with quantifying, placement and setting up of APs according to both area coverage and performance criteria. In Fault Response phase we consider the reconfiguration of the active APs in order to deal with AP fault in the service area.

In future work the implementation of the proposed algorithm will be done using Network Simulator-2, and various simulation results will be studied and compared with the existing algorithms. Adding restoration of the previous configuration after the failed AP is corrected and restored will enhance the algorithm.

REFERENCES

[1] Flavio E. de Deus, Ricardo Staciarini Puttini, Luis Fernando Molinaro, Joseph Kabara; "On Survivability of IEEE 802.11 WLAN"; Proceedings of the IEEE International Conference on Sensor Networks, Ubiquitous, and Trustworthy Computing; 2006.

[2] A.P. Snow, U. Varshney, and A. D. Malloy. "Reliability and survivability of wireless and mobile networks". IEEE Computer, 49–55, July 2000.

[3] "Configuring a Wireless Distribution System (WDS) with the 3Com OfficeConnect Wireless 11a/b/g Access Point" [online]. Available:"www.3com.com/other/pdfs/products/en_US/104108.pdf".

[4] D. Tipper, T. Dahlberg, H. Shin, and C. Charnsripinyo. "Providing fault tolerance in wireless access networks". IEEE Communications, 62–68, January 2002.

[5] Rajeev Gandhi; "Tolerance to Access-Point Failures in Dependable Wireless Local-Area Networks"; Proceedings of the Ninth IEEE International Workshop on Object-Oriented Real-Time Dependable Systems; 2004.

[6] Z. J. Haas and Y.-B. Lin. "Demand re-registration for PCS database restoration". Mobile Networks and Applications, 191–198, 2000.

[7] D. Tipper, S. Ramaswamy, and T. Dahlberg. "PCS network survivability". Mobile and Wireless Communication Networks conference, September 1999.

[8] "WDS (Wireless Distribution System)"; ORiNOCO Technical Bulletin 046/ A; February 2002.

[9] Wireless Local Area Network (WLAN) Explained [online]. Available: http://www.anthonycairns.com/Explained/Items_Explained_WLAN.htm

[10] Manmath Narayan Sahoo, Pabitra Mohan Khilar, *"Survivability of IEEE 802.11 Wireless LAN Against AP Failure"*, International Journal of Computer Applications in Engineering, Technology and Sciences (IJ-CA-ETS), pp.424-428, April, 2009.

[11] D. Chen, C. Kintala, S. Garg, and K. S. Trivedi. "Dependability enhancement for IEEE 802.11 wirelessLAN with redundancy techniques". Proceedings of the International Conference on Dependable Systems and Networks, 521–528, June 2003