INTERNATIONAL JOURNAL OF COMPUTER APPLICATIONS IN ENGINEERING, TECHNOLOGY AND SCIENCES (IJ-CA-ETS)

SURVIVABILITY OF IEEE 802.11 WIRELESS LAN AGAINST AP FAILURE

[1]Manmath Narayan Sahoo, [2]Pabitra Mohan Khilar

[1,2]NIT Rourkela/CSE, Rourkela, India
[1]sahoo.manmath@gmail.com, [2]pmkhilar@nitrkl.ac.in

ABSTRACT:
In IEEE 802.11 WLAN, if an access-point fails, some or all the mobile stations connected to the network via the 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 fault in the service area.

KEYWORDS: Access points, Wireless Distributed System, Basic Service Set, Extended Service Set

1. INTRODUCTION

Wireless networks have been growing rapidly in the past years to support increasing demands for mobile communications. Thus WDS is normally used in large, open areas where pulling wires is cost prohibitive, restricted or physically impossible.
In IEEE 802.11 terminology a "Distribution System" **[8]** is system that interconnects so-called Basic Service Sets (BSS). A BSS is best compared to a "cell", driven by a single Access Point. A WDS link can be a point-to-point link **[3]** in which an access point can be wirelessly connected to at most one other access point otherwise it can be of point-to-multipoint type **[3]** in which an access point can be wirelessly connected to several other access points. 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. In particular, we focus on the problem of overcoming these AP's failures working with neighbor's MAC address and establishing a new path dynamically.
The reminder of the paper is organized as follows: section 2 presents the architecture of WLAN and describes different components of it. Section 3 outlines the related work that has been done in this area. In section 4 we present our proposed algorithm along with a worked example. Section 5 concludes our research work and gives future research directions.

2. WLAN ARCHITECHTURE

Figure 1 depicts various components of Wireless LAN which are described below.

2.1. 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).

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

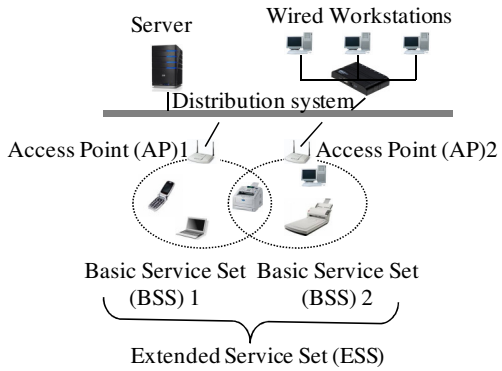

Figure 1 - Wireless LAN Architecture

2.3. 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.

2.4. SSID (Service Set Identifier)

A service set identifier or SSID **[10]**, is a name used to identify the particular 802.11 WLAN to which a user wants to attach i.e. It distinguishes one WLAN from other.

2.5. 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.

2.6. 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.

3. RELATED WORK

Rajeev Gandhi **[5]** describes a redundancy technique to tolerate access-point failures in wireless networks by using additional access-point designated as a backup, and that can be 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.

4. 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.

4.1. 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.

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 nodes 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
```

Figure 2 - Algorithm for establishing route

4.2. 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: Apply DFS to the spanning tree and store the traversing sequence in an array DFS[ ].
Step 2: Find failure node applying ping between starting node and the node in DFS[ ]. Get the just previous node P of the failure node. Let T=P.

Step 3:

```
while(all active nodes aren't connected)
continue
   Find adjacency list L of node P from
   modified adjacency matrix.
   Store MAC ID of nodes in L, in P's
   Neighbor[] iff it does not form a loop.
   If (P.next[1]=null in BFS[] sequence) then
      P=start of BFS[].
   Else if (P.next ≠ T) then
         P=P.next.
      Else
         exit.
      End if
   End if
End while
```

4.3. Worked Example
Algorithm for Establishing Route
Step 1: The complete graph for 7 APs is shown in Fig 4 along with the initial weight adjacency matrix in Table I.

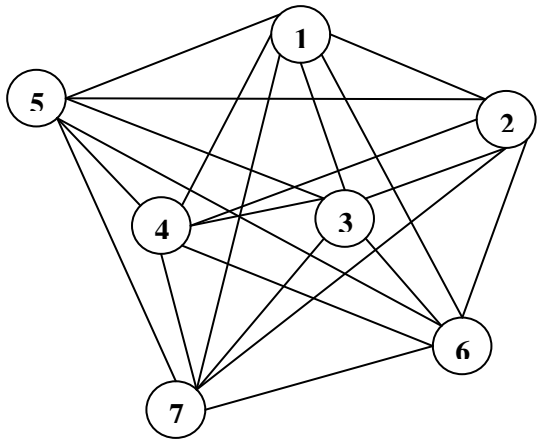

Figure 4 - Complete graph for Access Point network

[1]P.next accesses the next node in the array after P.

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	6
4	9	8	5	0	5	12	8
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 Fig 5.

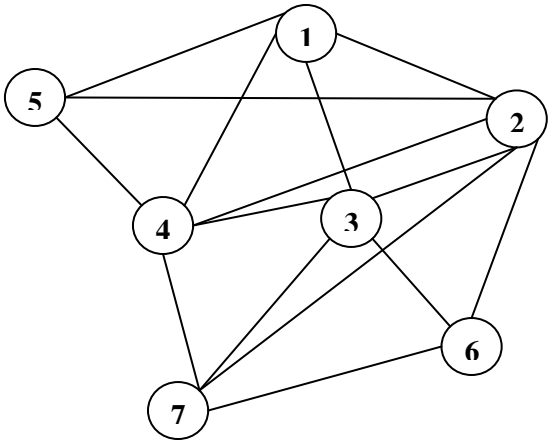

Figure 5 - Modified graph after pruning against threshold value

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	6
4	9	8	5	0	5	0	8
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 Fig 6.

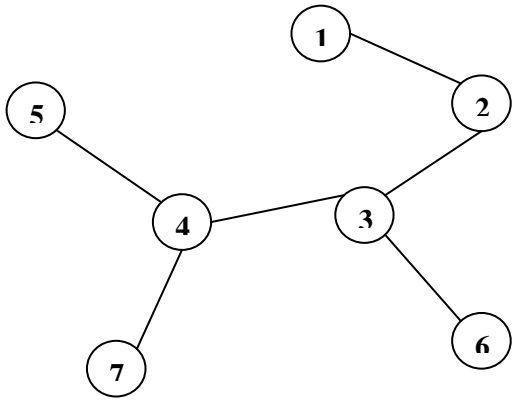

Figure 6 - Minimum spanning tree of the modified graph

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

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

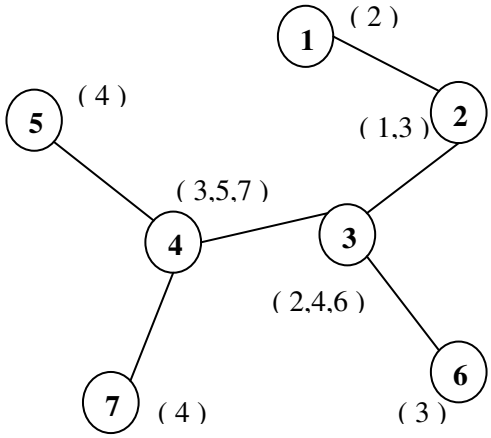

Figure 7 - Access points with neighbor MAC IDs

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

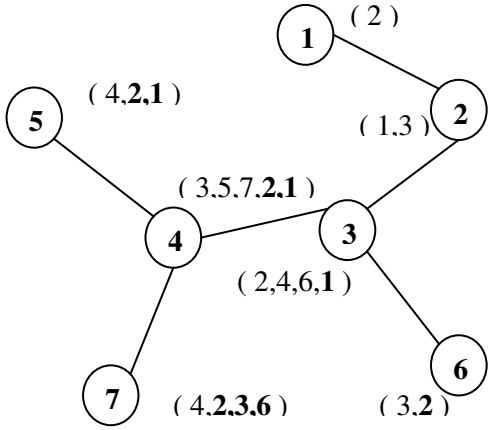

Figure 8 - Access Points with neighbor and redundant MAC ID

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.

The just previous node to AP 2 is AP 1. So P=1 and T=1.

Step 3: The adjacency list of P in BFS sequence is 5,3,4 (AP 2 is not included because AP 2 is failed).

By placing 5 as the neighbor of P (=1) all the active APs become connected and it does not lead to loop formation. Figure 9 shows the final network after network survival.

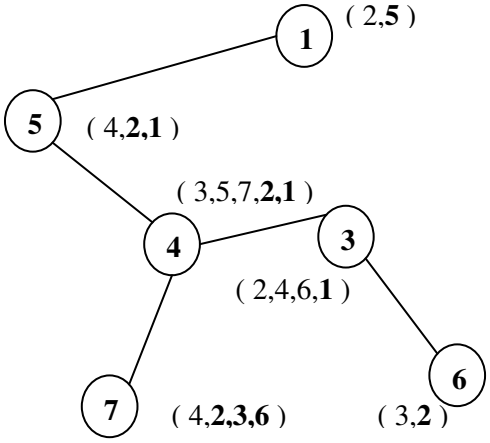

Figure 9 - Final network after network survival

5. CONCLUSION

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.

6. 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. *Service Set Identifier [online]. Available: http://wapedia.mobi/en/Service_set_identifier*
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.*