ISSN 2250-3153

Automatic Reconfiguration in Wireless Mesh Networks Using Static and Dynamic IP Allocations with Security Considerations

Mrs. Sarika.S and Mrs. S.Dhanalakshmi

Dept.of Electronics and Communication
K.S.R.College of Engineering
Tiruchengode,Tamil Nadu-637 215, India

Abstract- The demands for the network usage are increasing day by day. Result of this is the interference between users and many such losses, which may degrade the system performance. Security techniques could be incorporated to give the ultimate protection to the entire network. The existing techniques like cryptography make the system complicated. This paper is going to deal with a system which can automatically reconfigure the wireless mesh network (WMN). Necessary changes are made in local and radio channel assignments for failure recovery. From the changes made the system make appropriate reconfigurations in the settings of the network. A WMN with an IEEE standard 802.11 along with a Microsoft Visual Studio-10 based evaluation is done. Along with this security is introduced by making use of the dynamic routing which reduces the complexity of security implementation. This routing algorithm can in turn randomize the delivery path of data transmission.

Index Terms-Self reconfiguration,Wireless Mesh networks IEEE 802.11, dynamic routing, link-failures, security, and sensor selection.

I. INTRODUCTION

Wireless mesh networks, an emerging technology, may bring the dream of a seamlessly connected world into reality. Wireless mesh networks can easily, effectively and wirelessly connect entire cities using inexpensive, existing technology. Traditional networks rely on a small number of wired access points or wireless hotspots to connect users. In a wireless mesh network, the network connection is spread out among dozens or even hundreds of wireless mesh nodes that "talk" to each other to share the network connection across a large area. Mesh nodes are small radio transmitters that function in the same way as a wireless router. Nodes use the common WiFi standards known as 802.11a, b and g to communicate wirelessly with users, and, more importantly, with each other. Nodes are programmed with software that tells them the way to interact within the larger network. A system which can adapt to failures by automatic reconfiguration is thus introduced [1].

Security has become one of the major issues for data communication over wired and wireless networks. Different from the past work on the designs of cryptography algorithms and system infrastructures another method to provide security through routing is to be implemented [2], [3].Dynamic routing protocols are supported by software applications running on the routing device (the router) which dynamically learn network destinations and how to get to them and also advertise those destinations to other routers. This advertisement function allows all the routers to learn about all the destination networks that exist and how to reach those networks. To implement such dynamic routing protocols, each device needs to communicate routing information to other devices in the network. Each device then determines what to do with the data it receives — either pass it on to the next device or keep it, depending on the protocol. The routing algorithm used should attempt to always ensure that the data takes the most appropriate fastest route to its destination [2].

Maintaining the performance of WMNs in the face of dynamic link failures remains a challenging problem. The quality of wireless links in WMNs can degrade (i.e., link-quality failure) due to interference in other collocated wireless networks. Links in some areas may not be able to accommodate increasing QoS demands from end-users (QoS failures), depending on spatial or temporal locality. Links in some areas may not be able to access wireless channels during a certain time period (spectrum failures) due to spectrum etiquette [4]. Next, the network runs routing protocols to determine the path of the admitted flows. This routing protocol is also assumed to include route discovery and recovery algorithms that can be used for maintaining alternative paths even in the presence of link failures.

As wireless sensor networks continue to attract attention for use in numerous commercial and military applications, there have been many efforts to improve their energy efficiency so that they can operate for very long periods with no manual maintenance. Because of the limited energy supplies of typical micro sensors, however, achieving long network lifetimes has been a very challenging task. Since the cost of manufacturing sensor nodes continues to decrease and large-scale networks consisting of thousands of sensors become realizable, the redundancy that exists among the data generated by the sensors can be exploited. Recent work in this area has focused on techniques such as dynamic sensor selection, in-network aggregation, and distributed source coding that reduce the amount of data generated by the network but ensure that the cumulative data from the sensor network at any given time meets

the sensor network's application quality of service (QoS) requirements.

In this work, Dynamic Antenna Range and Packet aware Routing (DAPR), is proposed which is an integrated routing and sensor selection protocol for wireless sensor networks that attempts to avoid these critical sensors by assigning novel routing costs that incorporate coverage overlap and choose sensors to actively sense and generate data with the knowledge of the effects that this has on potential routers. Routing costs are the first parameter that is to be attempted to avoid routing through sensors that are critical in the sense of meeting application QoS requirements. Sensors are used to sense the various parameters in the network. Here no hardware unit is used. Instead of that software or otherwise coding is written for the working of the sensor part.

II. NETWORK MODEL

The network is assumed to be consisting of mesh nodes, wireless links and gateway. Multi-radio mesh refers to a unique pair of dedicated radios on each end of the link. This means there is a unique frequency used for each wireless hop and thus a dedicated CSMA collision domain. This is a true mesh link where maximum performance without bandwidth degradation in the mesh and without adding latency can be acheived. Such a WMN is shown in Figure1.

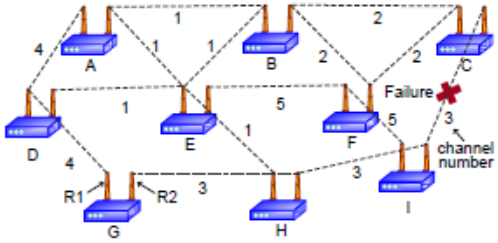

Figure 1: Multi –radio WMN, which has an initial channel assignment as shown

A. *Drawbacks of existing approaches*

Earlier approaches confine the network changes to be as local as possible. It cannot opt for entire network settings. Even though the approach called greedy channel assignment resolves the above drawback it still has ripple effects which result in the neighboring node settings even if a local change occurs. While considering the QoS, the channel and scheduling algorithms can provide optimal configurations in the network. But this may result in network disruptions. Cross layer interaction can reduce the detouring overhead but has to take extra care in reducing the interference [5]-[10]. Existing work on security-enhanced data transmission includes the design of cryptography algorithms, system infrastructures and security-enhanced routing methods. Their common objectives are often to defeat various threats over the Internet, including eavesdropping, spoofing, session hijacking, etc. All such security treatments make the entire network implementation complicated [3].The existing systems can only deal with large organizations and cannot deal with small ones. Static IP allocation along with dynamic allocation makes the system applicable in small as well as large organizations.

B. *Architecture of ARS*

The algorithm given below describes steps follows by the ARS.

Monitoring period (t_m)

1: for every link j do

2: measure link-quality (l_q) using passive monitoring;
3: end for
4: send monitoring results to a gateway g;

Failure detection and group formation period (t_f)
5: if link l violates link requirements r then
6: request a group formation on channel c of link l;
7: end if
8: participate in a leader election if a request is received;

Planning period (M, t_p)

9: if node i is elected as a leader then
10: send a planning request message (c, M) to a gateway;
11: else if node i is a gateway then

12: synchronize requests from reconfiguration groups M_n

13: generate a reconfiguration plan (p) for M_i;

14: send a reconfiguration plan p to a leader of M_i;
15: end if

Reconfiguration period (p, t_r)
16: if p includes changes of node i then
17: apply the changes to links at t;
18: end if
19: relay p to neighboring members, if any.

The monitoring period indicates that whether we are in a network or not otherwise monitoring period implies the period for which it will take the system to get monitored. The results of this will be time. During the failure detection and group formation period, the s/m under same operating system will be brought into same groups, so that a common access can be given to all. Important term to detect the failure is time to live (TTL). Requesting a group formation on channel c of link will be helping in such a way that, if a power failure occurs in one node neighbors can be asked for clarification to take further steps. The explanations of the steps are given in [1].

ARS undergo localized reconfiguration [8] together with the QoS [5], [6], [11] aware planning. Autonomous reconfiguration is done only after monitoring the link quality. To include rerouting for the reconfiguration planning, the prescribed system interacts across the network and link layers [9],[10].The flow chart shown in Figure 2 gives the diagrammatic explanation of the entire work. The diagrammatic representation of the steps to be followed is shown in Figure 2. Distance vector –based algorithm is used for dynamic routing.

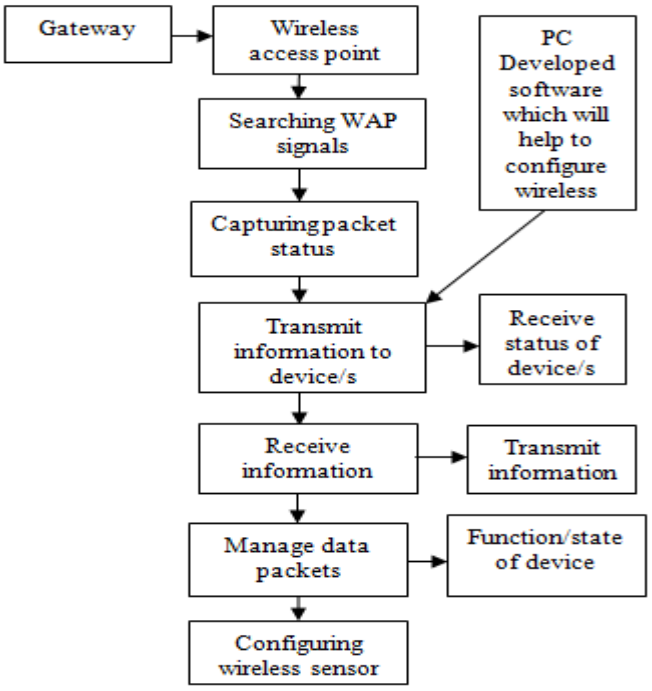

Figure 2: Process flow

A dynamic routing algorithm that could randomize delivery paths for data transmission is proposed here. The algorithm is easy to implement and compatible with popular routing protocols, such as the Routing Information Protocol in wired networks and Destination-Sequenced Distance Vector protocol in wireless networks, without introducing extra control messages. In previous systems such messages were present. Dynamic routing describes the capability of a system, through which routes are characterized by their destination, to alter the path that the route takes through the system in response to a change in conditions. The adaptation is intended to allow as many routes as possible to remain valid (that is, have destinations that can be reached) in response to the change.

C. Functions of ARS

ARS undergo localized reconfiguration together with the QoS aware planning. ARS systematically generates the reconfiguration plans into three processes like feasibility, satisfiability and optimality together with different constraint levels. The constraints used are connectivity, QoS demands and utilization. The plans thus formulated should be feasible since they are necessary to search all the required link changes in a faulty area.

The initial step to be done by the ARS is to detect the faulty links or channels. The system considers three primitive link changes S R and D. Channel switch S is used to simultaneously change the tuned channel, radio switch R is used to to switch and associate one radio in node A with another in B. Routing switch D is to redirect the traffic along the faulty link to another path. ARS follows a two-step approach-generation of feasible plans per link using the primitives and then combines a set of feasible plans that enable a network to maintain connectivity.

III. SYSTEM IMPLEMENTATION

The software architecture of ARS is shown in Figure 3.

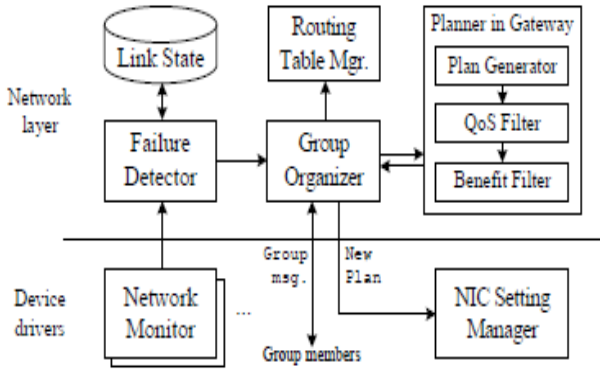

Figure 3: Software architecture of ARS

The software specification can be describes as follows:

A. Front End

Microsoft Visual studio 2010 is used in this project
Platform: Windows XP or later Versions
Programming language: C SHARP.Net

B. Features

Microsoft Visual Studio is an integrated development environment (IDE) from Microsoft. It is used to develop console and GUI with Windows applications, web sites, web application, and web services for all platforms supported by Microsoft Windows, Windows Mobile, .NET Framework, and .NET Compact Framework. The result to be achieved is seen in the Microsoft Visual Studio-10 window.

IV. SECURITY CONSIDERATIONS

The aim is to propose a dynamic routing algorithm to improve the security of data transmission. The eavesdropping avoidance problem can be defined as follows:
Given a graph for a network under discussion, a source node, and a destination node, the problem is to minimize the path similarity without introducing any extra control messages, and hence reduce probability of eavesdropping consecutive packets over a specific link.

Rely is on existing distance information exchanged among neighbouring nodes which can also be routers for the seeking of routing paths. In many distance-vector-based implementations, e.g., those based on Routing Information Protocol, each node N_i maintains a routing table in which each entry is associated with a tuple (t, $W_{N_i,t}$,Next hop), where t, $W_{N_i,t}$, and Next hop denote some unique destination node, an estimated minimal cost to send a packet to t, and the next node along the minimal-cost path to the destination node, respectively.For secured dynamic routing an extended routing table is needed.

The algorithm considered for the security in this paper, Distributed Dynamic Routing Algorithm (DDRA), consists of two parts:
1. Randomizer process for packet deliveries
2. Maintenance of extended routing table.
Consider the delivery of packets with destination t at a node Ni. To reduce or avoid eves-dropping the following algorithm is used. Among these nodes the packets are randomized. For that certain procedures are needed. The algorithms for the above two processes are shown below.

A. *Randomized selector*

1: Let h_s be the used next hop for the previous packet delivery for the source node s
2: if $h_s \in C_t^{N_i}$ then
3: if $|C_t^{N_i}| > 1$, then
4: randomly choose a node x from $\{C_t^{N_i} - h_s\}$ as a next hop, send the packet pkt to node x.
5: $h_s \leftarrow$ x and update routing table of N_i
6: else
7: send pkt to h_s
8: end if
9: else
10: randomly choose node y from $C_t^{N_i}$ as a next hop and send pkt to y
11: $h_s \leftarrow$ y, and update the routing table of
12:end if

For the routing table maintenance the distance vectors have to be taken into consideration. The distance vectors can be exchanged among the adjacent nodes based on predefined time duration.

B. *Maintenance of routing table*

1: if the destination node t is not in the routing table then
2: add the entry (t, $(w_{N_i,N_j} + W_{N_j,t})$, $C_t^{N_i} = \{N_j\}$, $H_t^{N_i} = \varnothing$)
3: else if $(w_{N_i,N_j} + W_{N_j,t}) < W_{N_i,t}$,then
4: $C_t^{N_i} \leftarrow$,$(w_{N_i,N_j} + W_{N_j,t})$, and is marked as the minimal cost next hop
5: $W_{N_i,t} \leftarrow (w_{N_i,N_j} + W_{N_j,t})$
6: foe each node $N_k \in Nbr_i$ except N_j do
7: if $W_{N_k,t} < W_{N_i,t}$, then
8: $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_k\}$
9: end if
10: end for
11: send (t, $W_{N_i,t}$) to each neighboring node
$N_k \in Nbr_i$
12: else if $(w_{N_i,N_j} + W_{N_j,t}) > W_{N_i,t}$ then
13: if ($N_j \in C_t^{N_i}$) then
14: if was marked as the minimal cost next hop then
15: $W_{N_i,t} \leftarrow MIN_{N_k \in N_{br_i}} (w_{N_i,N_k} + W_{N_k,t})$
16: $C_t^{N_i} \leftarrow \varnothing$
17: for each node $N_k \in Nbr_i$ do
18: if $W_{N_k,t} < W_{N_i,t}$ then,
19: $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_k\}$
20: end if
21: end for
22: send (t, $W_{N_i,t}$) to each neighboring node
23: else if $W_{N_j,t} > W_{N_i,t}$, then
24: $C_t^{N_i} \leftarrow C_t^{N_i} - \{N_j\}$
25:end if
26: else if ($N_j \notin C_t^{N_i}$) $\wedge$ ($W_{N_j,t} < W_{N_i,t}$) then
27: $C_t^{N_i} \leftarrow C_t^{N_i} \cup \{N_j\}$
28: end if
29: end if

V. RESULT

The effectiveness in meeting the varying QoS requirements in a multi radio wireless mesh network is evaluated. We initially assign the link capacities symmetrically. Available capacity of the ARS is increased via reconfiguration. The dynamic routing introduced gives security to the routed packets. The steps followed in the entire ARS processing and the associated results are shown in figures 4 and 5 and the security incorporated output is shown in Figure 6. The results shown are results viewed in the Microsoft Visual Studio -10 window. These are formed by using the networks available in the system used.

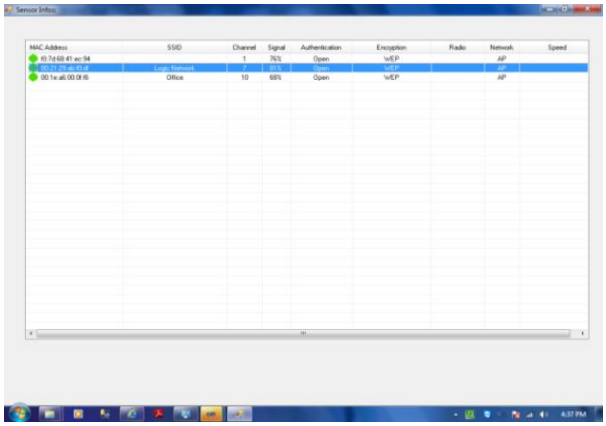

Figure 4: Retrieving the access points

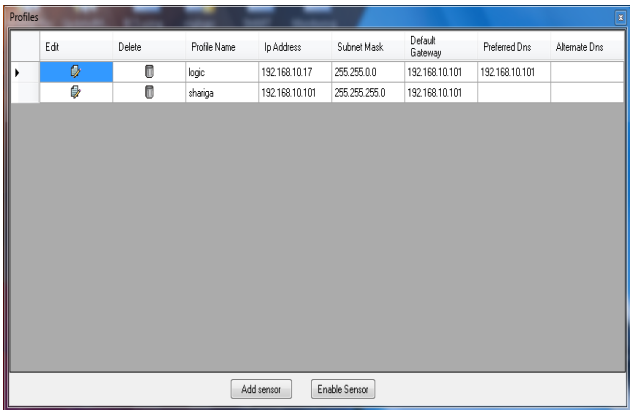

Figure 5: Creation of profile

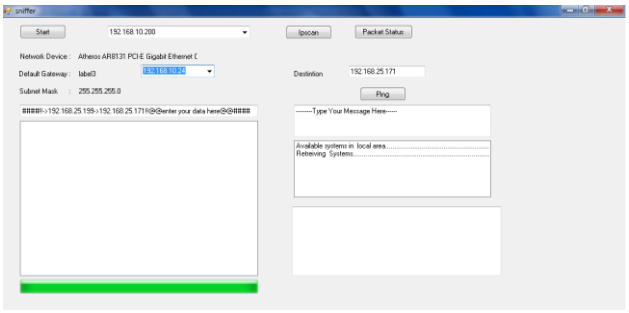

Figure 6: Security incorporated result

VI. CONCLUSION

This paper represents a system which automatically reconfigures the wireless mesh networks. Only local configuration changes are required in this method. This change is done by properly exploiting the radio and channel diversities. Thus the ARS detects real-time failure and reconfigures the network thereby increasing the channel efficiency. The dynamic routing reduces the complexity which was present in the previous cryptographic based systems. Since both the IP allocations are used this system can be used for large and small organizations.

REFERENCES

[1] Kyu-Han Kim and Kang G. Shin,"Self-Reconfigurable Wireless Mesh Networks IEEE/ACM Trans. on networking vol 19,no.2,April 2011

[2] Chin-Fu Kuo, Ai-Chun Pang and Sheng-Kun Chan," Dynamic Routing with Security Considerations IEEE Trans. on Parallel and Distributed systems,vol 20,no.1,January 2009.

[3] R. Thayer, N. Doraswamy, and R. Glenn, *IP Security Document Roadmap*, Request for comments (RFC 2411), Nov. 1998.

[4] M. J. Marcus, "Real time spectrum markets and interruptible spectrum: New concepts of spectrum use enabled by cognitive radio," in *Proceedings of IEEE DySPAN*, Baltimore, MD, Nov.2005.

[5] M. Alicherry, R. Bhatia, and L. Li, "Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks,"in *Proceedings of ACM MobiCom*, Cologne, Germany, Aug. 2005.

[6] M. Kodialam and T. Nandagopal, "Characterizing the capacity region inmulti-radio multi-channel wireless mesh networks," in *Proceedings ofACM MobiCom*, Cologne, Germany, Aug. 2005.

[7] A. Brzezinski, G. Zussman, and E. Modiano, "Enabling distributed throughput maximization in wireless mesh networks-a partitioning approach,"in *Proceedings of ACM MobiCom*, Los Angeles, CA, Sept.2006.

[8] A. Raniwala and T. Chiueh, "Architecture and algorithms for an IEEE 802.11-based multi-channel wireless mesh network," in *Proceedings ofIEEE InfoCom*, Miami, FL, Mar. 2005.

[9] S. Nelakuditi, S. Lee, Y. Yu, J. Wang, Z. Zhong, G. Lu, and Z. Zhang,"Blacklist-aided forwarding in static multihop wireless networks," in *Proceedings of IEEE SECON*, Santa Clara, CA, Sept. 2005.

[10] S.Chen and K. Nahrstedt, "Distributed quality-of-service routing in adhoc networks," *IEEE JSAC*, vol. 17, no. 8, 1999.

AUTHORS

First Author – Mrs.Sarika.S, Dept. of Electronics and Communication, K.S.R.College of Engineering, Tiruchengode,Tamil Nadu-637 215
Email ID: sharika_sankar@yahoo.com
Second Author – Mrs.S.Dhanalakshmi, Assistant Professor(Sr.) Dept..of Electronics and Communication, K.S.R.College of Engineering, Tiruchengode,Tamil Nadu-637 215
Email ID : dhanaece45@gmail.com