International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 06 Issue: 05 | May 2019 www.irjet.net p-ISSN: 2395-0072

REDUCTION OF PACKET DATA LOSS IN WIRELESS MESH NETWORK USING PATH MECHANISM APPROACH

Rohit Bansal[1], Manpreet Kaur[2], Vishal Garg[3]

[1, 2, 3] Department of Electronics & Communication Engineering
[1, 2, 3] *Swami Vivekanand Institute of Engineering and Technology, Banur, INDIA*

Abstract - *A wireless mesh network (WMN) is a communication network made up of radio nodes organized in a mesh topology. Wireless mesh network often consists of mesh clients, mesh routers and gateways. A wireless Mesh network uses multi-hop communication. Due to multi-hop architecture and wireless nature, Mesh networks are vulnerable to various types of Denial of Services attack. It suffers from Packet dropping at Routing layer. Client nodes are unable to get services from gateway nodes, hence network gets down. The Paper emphasis on the developing of a path protocol when the minimum possible packet drop occurs in wireless mesh networks. Due to packet dropping occurrences the network performance degrades. In the work, we have evaluated the Performance of WMN under packet dropping on the basis of their throughput and Data packet loss.*

Key Words: WMN; Packet Loss, Path Dropping, PDA

1. INTRODUCTION

Wireless mesh networking has emerged as a promising concept to meet the challenges in next-generation wireless networks such as providing flexible, adaptive, and reconfigurable architecture while offering cost-effective solutions to service providers. Several architectures for wireless mesh networks (WMNs) have been proposed based on their applications [1]. One of the most general forms of WMNs interconnects the stationary and mobile clients to the Internet efficiently by the core nodes in multi-hop fashion. The core nodes are the mesh routers which form a wireless mesh backbone among them. The mesh routers provide a rich radio mesh connectivity which significantly reduces the up-front deployment cost and subsequent maintenance cost. They have limited mobility and forward the packets received from the clients to the gateway router which is connected to the backhaul network/Internet [2].

The mesh backbone formed by mesh routers provides a high level of reliability [3]. WMNs are being considered for a wide variety of applications such as backhaul connectivity for cellular radio access networks, high-speed metropolitan area mobile networks, community networking, building automation, intelligent transport system networks, defence systems, and citywide surveillance systems. Prior efforts on wireless networks, especially multi-hop ad hoc networks, have led to significant research contributions that range from fundamental results on theoretical capacity bounds to development of efficient routing and transport layer protocols [4]. However, the recent work is on deploying sizable WMNs and other important aspects such as network radio range, network capacity, scalability, manageability, and security. There are a number of research issues in different layers of the protocol stack and a number of standards are coming up for the implementation of WMNs for WANs, MANs, LANs, and PANs. The mesh networking test beds by industries and academia further enhanced the research in WMNs. The mesh networking products by different vendors are making WMNs a reality [5].

1.1 Architecture of WMN

There are two types of nodes in a WMN called mesh routers and mesh clients. Compared to conventional wireless routers that perform only routing, mesh routers have additional functionalities to enable mesh networking. The mesh routers have multiple interfaces of the same or different communications technologies based on the requirement. They achieve more coverage with the same transmission power by using multi hop communication through other mesh routers. They can be built on general-purpose computer systems such as PCs and laptops, or can be built on dedicated hardware platforms (embedded systems). There are a variety of mesh clients such as laptop, desktop, pocket PCs, IP phones, RFID readers, and PDAs. The mesh clients have mesh networking capabilities to interact with mesh routers, but they are simpler in hardware and software compared to mesh routers. Normally they have a single communication interface built on them. The architecture of WMNs (shown in Figure 1) is the most common architecture used in many mesh networking applications such as community networking and home networking. The mesh routers shown have multiple interfaces with different networking technologies which provide connectivity to mesh clients and other networks such as cellular and sensor networks. Normally, long-range communication techniques such as directional antennas are provided for communication between mesh routers. Mesh routers form a wireless mesh topology that has self-configuration and self-healing functions built into them. Some mesh routers are designated as gateways which have wired connectivity to the Internet. The integration of other networking technologies is provided by connecting the BS of the network that connects to WMNs to the mesh routers. Here, the clients communicate to the BS of its own network and the BS in turn communicates to the mesh router to access the WMN.

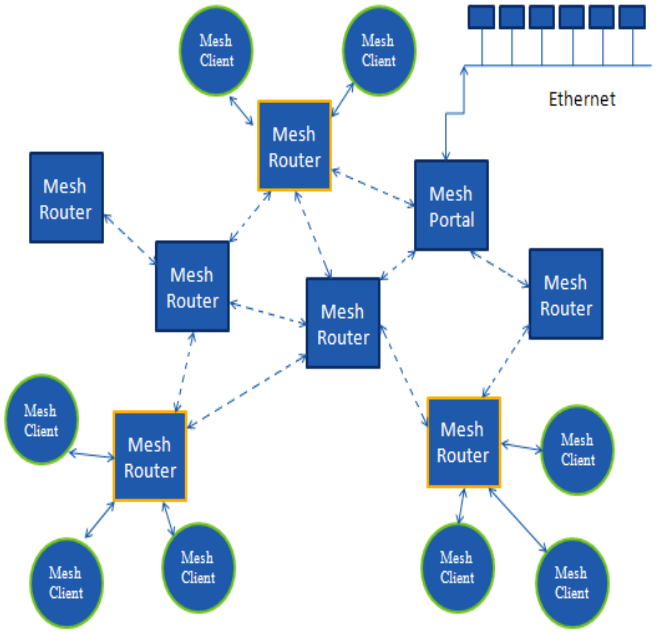

Figure 1: Wireless Mesh Network

1.2 Applications of WMNs

WMNs introduce the concept of a peer-to-peer mesh topology with wireless communication between mesh routers. This concept helps to overcome many of today's deployment challenges, such as the installation of extensive Ethernet cabling, and enables new deployment models. Deployment scenarios that are particularly well suited for WMNs include the following [6]:

- Campus environments (enterprises and universities), manufacturing, shopping centres, airports, sporting venues, and special events
- Military operations, disaster recovery, temporary installations, and public safety
- Municipalities, including downtown cores, residential areas, and parks
- Carrier-managed service in public areas or residential communities

Due to the recent research advances in WMNs, they have been used in numerous applications. The mesh topology of the WMNs provides many alternative paths for any pair of source and destination nodes, resulting in quick reconfiguration of the path when there is a path failure. WMNs provide the most economical data transfer coupled with freedom of mobility. Mesh routers can be placed anywhere such as on the rooftop of a home or on a lamppost to provide connectivity to mobile/static clients. Mesh routers can be added incrementally to improve the coverage area. These features of WMNs attract the research community to use WMNs in different applications:

Home Networking: Broadband home networking is a network of home appliances (personal computer, television, video recorder, video camera, washing machine, refrigerator) realized by WLAN technology. The obvious problem here is the location of the access point in the home, which may lead to dead zones without service coverage. More coverage can be achieved by multiple access points connected using Ethernet cabling, which leads to an increase in deployment cost and overhead. These problems can be solved by replacing all the access points by the mesh routers and establishing mesh connectivity between them. This provides broadband connectivity between the home networking devices and only a single connection to the Internet is needed through the gateway router. By changing the location and number of mesh routers, the dead zones can be eliminated. Figure 2 shows a typical home network using mesh routers.

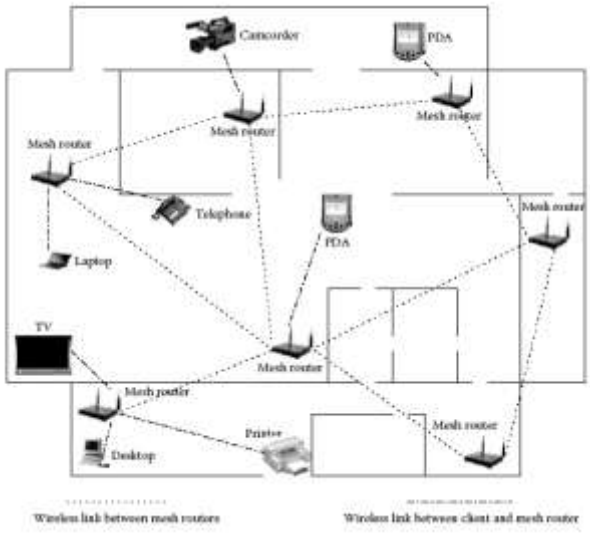

Figure 2: Wireless mesh network-based home networking

2. LITERATURE REVIEW

N.A Benjamin et al, 2016 proposed that WMNs can be used to transmit vital information arising from the wireless body sensor network (WBSN) to a backbone network. The integration of WBSN and WMN technologies results in wireless sensor mesh network (WSMN) and this type of network can be utilized for remote health monitoring of patients. The battery-powered, memory-constrained sensors transmit the sensed information to their nearest mesh nodes and the mesh nodes, in turn, use multi-hop routing to transmit the information to the backbone network devices like PDA or the servers for health monitoring applications. The authors have investigated performance of such a WSMN for patient health monitoring applications, in terms of parameters like delay, and throughput under varying number of patients and doctors [7].

Sukla Banerjee, 2010 proposed a mechanism to detect and remove the black hole and gray hole attacks. This technique is capable of cooperating malicious nodes which drop a significant fraction of packets in AODV protocol. In this technique, each node can locally maintain its own table of black listed nodes whenever it tries to send data to any

destination node and it can also aware the network about the black listed nodes [8].

Y.L Sun et al, 2016 have presented trust as a measure of uncertainty. Using theory of entropy, the authors have developed a few techniques to compute trust values from certain observation. In addition, trust models – entropy-based and probability-based are presented to solve the concatenation and multi-path trust propagation problems in a MANET [9].

Yu Cheng et al, 2009 proposed a practical algorithm channel aware detection (CAD) to detect and isolate the selective forwarding attackers in the area of multi hop networks such as WMNs. CAD mainly adopts two strategies for detection [10]

3. PROBLEM STATEMENT

Client nodes are unable to get services from gateway nodes, hence network gets down. The paper emphasis on the developing of a path protocol when the minimum possible packet drop occurs in wireless mesh networks. Due to packet dropping occurrences the network performance degrades. In the work, we have evaluated the Performance of WMN under packet dropping on the basis of their throughput and Data packet loss.

3.1 Objectives

The objectives of the thesis are summarized as follows:

- Analysis of performance due to packet dropping attacks in wireless mesh networks at Routing Layer.
- Propose a detection Technique.
- Implementation of Proposed Technique using MATLAB

4. CONCLUSION

Client nodes are unable to get services from gateway nodes, hence network gets down. The paper emphasis on the developing of a path protocol when the minimum possible packet drop occurs in wireless mesh networks. Due to packet dropping occurrences the network performance degrades. In the work, we have evaluated the Performance of WMN under packet dropping on the basis of their throughput and Data packet loss. In the future directions, this work can be extended by using hundreds of nodes and we need to develop the Intrusion detection System (IDS) that also chooses the monitor by considering battery life parameter. It is important to consider congestion conditions of the nodes using information obtained from other layers before determining the nodes to be malicious. Also, detecting intrusions at different layers increases the information about the malicious nodes thus identifying these nodes more accurately.

REFERENCES

[1] X. Wang and A. O. Lim, "IEEE 802.11s wireless mesh networks: Framework and challenges," Ad Hoc Netw., vol. 6, no. 6, pp. 970-984, 2008

[2] G. R. Hertz, S. Max, E. Weir, L. Berlemann, D. Denteneer, and S. Mangold, "Mesh Technology enabling Ubiquitous Wireless Networks," in Proceedings of the 2nd Annual International Wireless Internet Conference (WICON '06), Boston, MA, USA: ACM, Invited Paper, pp. 11, August, 2006.

[3] Yan Zhang, Jun Zheng "Book Title:-Security in Wireless Mesh Networks".

[4] w.steven,jan kryus, kyeongsoo kim, juan carlos zuniga "802.11s tutorial overview of the amendment for wireless local area networking" in ieee802 plenary, Dallas , November ,2006.

[5] Akyildiz, I.F.; Xudong Wang "A Survey on Wireless Mesh Networks" in Communications Magazine, IEEE Volume 43, Issue 9, pp. S23 - S30, September 2005

[6] A. Pirzada and C. McDonald, "Establishing trust in pure ad hoc networks", in Proceedings of the 27th Australasian Conference on Computer Science, Vol. 26,pp. 181-199, 2004.

[7] N. A. Benjamin and S. Sankaranarayanan, "Performance of wireless body sensor based mesh An Efficient Algorithm for detection of Selfish Packet Dropping Nodes in Wireless Mesh Networks 369 network for health application", International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM), Vol 2, pp. 20 – 28,2016.

[8] Sukla Banerjee, "Detection/Removal of Cooperative Black and Gray Hole Attack in Mobile Ad-Hoc Networks", Proceedings of the World Congress on Engineering and Computer Science, WCECS 2010, San Francisco, USA.

[9] Y.L. Sun, W. Yu, Z. Han, and K.J.R. Liu, "Information theoretic framework of trust modeling and evaluation for ad hoc networks", IEEE Journal on Selected Areas in Communications, Vol. 24, pp. 305 – 317, 2016.

[10] Yu Cheng, Devu Manikantan Shila and Tricha Anjali, "Channel-Aware Detection of Gray Hole Attacks in Wireless Mesh Networks", Dept. of Electrical and Computer Engineering, Illinois Institute of Technology, Chicago, USA, 2009.