ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, Vol 8(15), 67729, July 2015 ISSN (Online) : 0974-5645

Efficient Load Sharing using Multipath Channel Awareness Routing in Mobile Ad hoc Networks

D. Jagadeesan[1*], S. Narayanan[2] and G. Asha[3]

[1]Department of Computer Science and Engineering, Sreenivasa Institute of Technology and Management Studies, Chittoor - 517127, Andhra Pradesh, India; djagadeesanphd@gmail.com
[2]Department of Computer Science and Engineering, Adhiparasakthi College of Engineering, Kalavai, Vellore District - 632 506, Tamil Nadu, India; sakthi.sakthinarayanan@gmail.com
[3]Department of Electronics and Communication Engineering, SCSVMV University, Kanchipuram - 631561, Tamil Nadu, India; ashajagadeesan@gmail.com

Abstract

Objectives: To develop a new multipath load sharing algorithm using channels sensing, node energy level analysis and malicious node detection. It aims at finding an efficient load sharing technique that gives better throughput delivery, less delay and security for data transformation. **Methods/Analysis:** A channel sensing between the nodes is performed to measure the signal to noise ratio and reject the path if the noise strength is greater than the signal strength. Prior energy level analysis is done for consistent data transmission over a period of time without any interrupt. A watchdog timer method is adopted for malicious node identification and removal. **Findings:** The quality of service in MANETs has been improved such as throughput has been increased 15% and packet delivery ratio has been increased 20% and the overall delay has been minimized 27%. **Conclusion/Application:** We proposed an efficient best path selection load sharing algorithm, which involves channel sensing, node energy level analysis and malicious node removal for security concern.

Keywords: Attacks, Channel Awareness, Channel Sensing, Load Sharing, Malicious, Noisy Path

1. Introduction

In[1,13] a Mobile Ad Hoc Network (MANET) consists in a group of wireless mobile nodes, which create short-term network in absence of relying on any offered infrastructure or centralized administration. In mobile ad hoc network presents lots of problems which are based Quality of Service. The target of QoS offered is to guarantee an improved delivery of data carried by the network, and an enhanced consumption of the network resources. One of the main aspects of the communications process is the design of the routing protocols used to create and sustain multi-hop routes to allow the communication of data between nodes. Thus routing is a crucial issue to the design of a MANETs. This is achieved by using some mechanism such as QoS routing to discover the best route which satisfies these necessities in the best manner.

2. Related Works

In[2] proposed Channel Aware Routing in MANETs with secure Hash Algorithm. SHA-1 algorithm was applied in CA-AOMDV protocol to attain secure routing in MANET. CA-AOMDV was used to generate stable link between source and destination. But there were still many problems such as tunneling attacks, selectively drop packets.

* Author for correspondence

In[3] proposed Routing-Aware Multiple Description Coding approach to support data transmission Over Mobile Ad-Hoc Networks with multiple path transport. A statistical model was constructed to estimate the packet loss probability of each packet transmitted over the network based on the standard ad hoc routing messages and network parameters. The frame loss probability was estimated and dynamically it selects reference frames to alleviate error propagation caused by the packet losses.

In[4] proposed On-demand Multipath Distance Vector Routing in Ad hoc Networks. AOMDV is a multipath extension to AODV. It uses link-disjoint, loop free paths. Loop freedom is ensured by accepting only lower hop-count alternate routes than the primary route. Intermediate nodes look at each copy of the RREQ to see if it provides a new node-disjoint path to the source. If it does, AOMDV updates its routes only if a reverse path can be set up. When all routes fail a new route discovery is broadcasted. The advantages are a fast and efficient recovery from failures. The main drawback is that path information used is often quite out of date because a new discovery process is initiated only when all the routes fail.

In[5] proposed Stable Link Based Multicast Routing Scheme for MANETs. Maximizing the link breakage time between two nodes within MANETs is very crucial for stable multicast routing. The authors considered node mobility and battery power ratio factors for stability of nodes. Link time between two nodes depended on both the factors. Selecting the routes between sources to multicast group depended on stability of nodes corresponding to neighbor. GPS system was used to get the coordinates of the nodes. The lack of link lifetime and energy efficient was not considered.

In[6] proposed Investigation of Adaptive Multipath Routing for Load Balancing[12] in MANETs. In this proposed work has balancing the load in a MANET is considered important because the nodes in MANET have limited communication resources such as bandwidth, buffer space, and battery power. So it is essential to distribute the traffic among the mobile host. Load balancing is used to increase throughput of the network. In this paper, some of the congestion removing and load balancing routing schemes have been surveyed. Also it is possible to maximize nodes lifetime, packet delivery ratio, and minimize traffic congestion and load unbalance, as a result, end-to-end packet delay can be minimized, and network performance in term of load can be balanced. The security issues due to malicious nodes and noise occurrence are not considered.

In[7] proposed a novel automatic security mechanism using SVM to defense against malicious attack occurring in AODV. The proposed method uses machine learning to categorize nodes as malicious. This system is far further resilient to the context changes general in MANET's, such as those due to malicious nodes changing their misbehavior patterns over time or quick changes in environmental factors, for instance the movement speed and communication range.

3. Problem Identification

- In single path routing all packets from source to destination travels along a same path, hence it requires high transmission power for those nodes involved in transmission.
- Since every packet has to be transmitted sequentially from source to destination along a single path that makes more delay for data transmission.
- Malicious node eventually may take part in the data transmission it causes packet drops and security problem.
- Due to radio link fluctuation that occurs in channel between nodes involved in transmission noisy data occurs at high rate.

4. Proposed Work

In MANETs, we proposed to transfer data packet between source and destination through multipath. This proposed scheme has to detect and remove the malicious nodes. Hence it reduces the packet loss and improves security. The channels between the nodes[8] are sensed and noisy paths are removed for efficient data transmission.

Figure 1 shows the discovery of all available paths between source and destination by the help of reactive routing protocol. Figures 2–5 examine individual path one by one and finds the best paths which has nodes whose energy level is greater than or equal to threshold value, no malicious nodes and noiseless channels.

4.1 Channel Sensing

The wireless channel is always vulnerable to radio link fluctuation hence it affect the data transmission over the channel. Our proposed system calculates the average

signal to noise ratio between the nodes. If signal strength is very much greater than noise then it select the channel otherwise it rejects the channel.

4.2 Malicious Node Detection

During the transmission of data packet any node act as a malicious node, due to this there should be occurrence of packet drop. Misbehavior node has to bear some energy costs in order to perform the thread. Malicious node can attack the network by masquerading and spoofing. Fabrication is an attack which is an authorized party not only gains the access and also insects counterfeit objects into the system. Fabrication performed by generating false routing messages (Gray hole attack). Gray hole attack is behave maliciously for some time duration by dropping packets after some time it may switch to normal behavior[9].

4.2.1 Black Hole Attack (Jellyfish Attack)

The black hole attack is an active insider attack, it has two properties:

- First, the attacker consumes the intercepted packets without any forwarding.
- Second, the node exploits the routing protocol, to announce itself as having an accurate route to a destination node, even though the route is counterfeit, with the intention of intercepting packets[10].
- First needs to intrude into the forwarding group and delays data packets unnecessarily. It result is end-to-end delay.

4.2.2 Worm Hole Attack

It is also known as tunneling attack. Tunneling attack is where two or more nodes may collaborate to encapsulate and exchange messages between them along existing data routes. Worm hole is one of most powerful attacks. In this type of attacks, the attacker disrupts routing by short circuiting the usual flow of routing packets. Wormhole attack can be done with one node also. But generally, two or more attackers connect via a link called "wormhole link"[11]. Wormhole attacks are relatively easy to deploy but may cause great damage to the network. Wormhole attack is a kind of replay attack that is particularly challenging in MANET to defend against. An attacker can tunnel a request packet RREQ directly to the destination node without increasing the hop-count value.

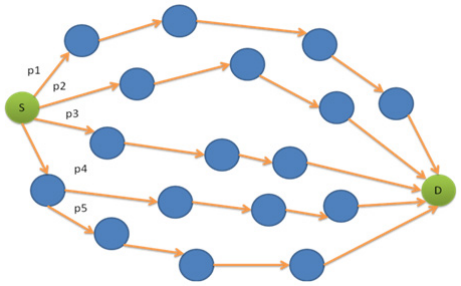

Figure 1. Discovery of available path (p1, p2, p3, p4 and p5).

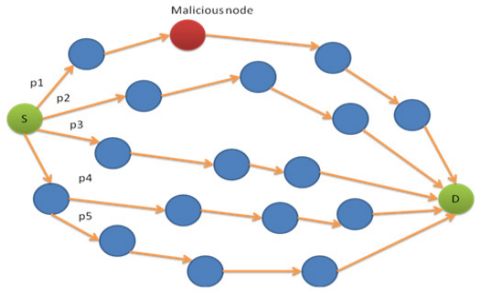

Figure 2. Identification of malicious node in the path (p1).

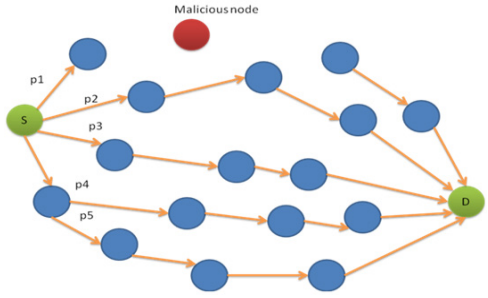

Figure 3. Remove the path involves malicious node (p1).

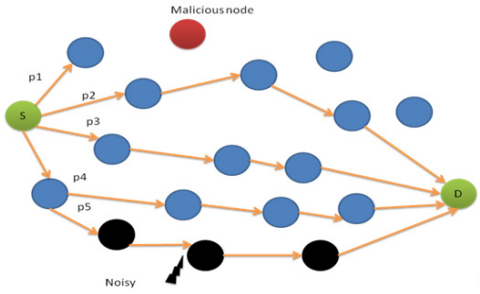

Figure 4. Identification of noise channel (p5) and remove the path.

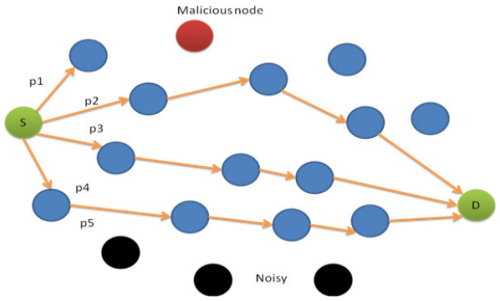

Figure 5. Available best path (p2, p3 and p4).

4.2.3 Algorithm for Selection of Best Paths

Discovery the N multipath channel using AOMDV;
Available path avail [N];
Start from source nodes;
Average threshold value TH_{avg};
Initialize i = 0, j = 0, n = s, count = 0;
While i< = N
Select the path avail [i];
L1: Sense the channel between n and next hop node (n+1);
If (channel signal > = TH_{avg}) then
    examine the n+1 node;
    if (n+1 node = malicious node or energy_level is low)
        reject the path;
        move to next path i++;
    else if (n+1 = destination)
        add best_path [count];
        i+ + and count++;
    else
        n++ ;
        go to L1;
    end if
else
    reject the path;
    move to next path i++;
end if
end while

4.2.4 Load Sharing

In multipath routing, the data packets can be sending to destination at various paths to reduce transmission power. Load sharing will reduce time consumption and more data packet can be send to destination at a time. Load sharing is used to push the traffic. In these techniques, network performance in terms of average delay and reliability. Load sharing is used to solve the problem like networks are highly loaded, large queue size, high packet delay, high packet loss ratio, high power consumption.

4.2.4.1 Algorithm for Load Sharing

Available best_path [count];
Available data packet p[packet_count];
Packet_count = number of data packet;
Initialize k = 0, j = 0;
while(k<packet_count)
    Send p[k] in best_path [j];
    k++;
    if (there is problem in the path)then
        count = count-1; // **To remove the path**
    end if
        j = j +1 mod count;

end while

5. Conclusion

In this paper, we propose a multipath based on selection of available best paths and load sharing algorithm. The selection criteria include sensing channel between the nodes and avoiding the noise path. It is a simple but effective algorithm to sharing the load and alleviates congestion in network. The algorithm results in reduction in the delay, overhead, minimizes traffic congestion and increase data transmission between source and destination with securely.

6. References

1. Tekaya M, Tabbane N, Tabbane S. Multipath routing with load balancing and QoS in Ad hoc Network. IJCSNS International Journal of Computer Science and Network Security. Aug; 10(8):280–6.
2. Rao PK, Vasundra S. Channel aware routing in MANETs with secure Hash Algorithm. International Journal of Scientific and Research Publications. 2012; 2(1):01–4.
3. Liao Y, Gibson JD. Routing-aware multiple description video coding over mobile ad-hoc networks. IEEE Transactions on Multimedia - TMM. 2011; 13(1):132–42.
4. Marina MK, Das SR. On-demand multipath distance vector routing in ad hoc networks. IEEE Proceedings of 9th International Conference on Network Protocols (ICNP); 2001 Nov. p. 14–23.
5. Kant K, Awasthi LK. Stable link based multicast routing scheme for MANET. IEEE Proceedings of International Conference on Computational Intelligence and Communication Networks (CICN); 2010. p. 296–300.

6. Sharma B, Chugh S, Jain V. Investigation of adaptive multipath routing for load balancing in MANET. IJEAT; 2013 Jun; 2(5):65–71.
7. Patel M, Sharma S. Detection of malicious attack in MANET a behavioral approach. Proceedings of IEEE International Conference on Advance Computing Conference (IACC); 2013. p. 388–93.
8. Ramprabu G, Nagarajan S. Design and analysis of novel modified cross layer controller for WMSN. Indian Journal of Science and Technology. 2015 Mar; 8(5):438–44.
9. Rajaram A, Palaniswami S. Malicious node detection system for mobile ad hoc networks.IJCSIT. 2010; 1(2):77–85.
10. Sharma R, Chanpreet Kaur C. Packet update scheme for prevention of blackhole attack in MANETs. Int J Adv Res Comput Sci Software Eng. 2013 Sep; 3(9):720–5.
11. Jhaveri RH, Patel AD, Parmar JD, Shah BI. MANET routing protocols and wormhole attack against AODV. International Journal of Computer Science and Network Security. 2010 Apr; 10(4):12–8.
12. Elnour MEE, Abd Latif MS, Isnin IF. Coarse grain load balance algorithm for detecting similar regions in dna and proteins sequences. Indian Journal of Science and Technology. 2014 May; 7(5):589–99.
13. Pillai MJ, Sebastian MP, Madhukumar SD. Dynamic Multipath Routing for MANETs – A QoS Adaptive Approach. IEEE Third International Conference on Innovative Computing Technology (INTECH); 2013. p. 308–13.