Detection and Removal of Packet Dropper Nodes for Congestion Control Over MANET

[1]Reeta Bourasi, [2]Sandeep Sahu
[1,2]SRIT

Abstract
Mobile Ad-Hoc network is wireless network of mobile nodes, with no centralized management and control. Network congestion has a severe impact on the throughput, routing and lifespan, etc. of a network. Packet dropper nodes have a major and worst impact in congestion over the MANET. Packet dropping nodes do not forward the incoming packets and may send the acknowledgement to the sender node. In this paper, we focus on the data packet dropping in Mobile Ad-hoc Network in both dense and a few node counts. The packet dropper nodes are eliminated using a new algorithm by adding a reliability factor of each node which is increased when the node receives the acknowledgement of the forwarded packet to assure that the node has actually forwarded the packet and have not dropped it. For showing the working of the algorithm, simulations has been created using NS2.

Keywords
MANET, Packet Dropper Nodes, Reliability

I. Introduction

Wireless Ad-Hoc network, with shared wireless channel to transmit messages, faces complicated wireless transmission environment, which will bring in a series of new problems, especially with routing, congestion being one of the problems. Generally speaking, for wireless Ad Hoc network, the calculation of the congestion control of one certain link should not just be based on the congestion of the link itself, instead, it should respond according to the general congestion message that interrupts the link. Therefore, to solve the routing congestion which might come up with the Ad Hoc network, the following issues should be taken into consideration:

- The intrinsic properties of wireless multiple-hop links
- The time varying of network topology
- Dynamic end users [1].

More and more advancements in wireless communication technologies and availability of less expensive, small, portable computing devices led to mobile computing and its applications. A "mobile ad hoc network" (MANET) [3] consists of mobile nodes connected by wireless links. The union of which forms an arbitrary graph. The nodes are free to move randomly thus, the network's topology may change rapidly and unpredictably. [2]

During the last few years Wireless mesh networking has become increasingly ubiquitous and the preferred mechanism to provide coverage to campuses, small towns, etc. In Wireless mesh networks a subset of the wireless nodes are connected to the wired backbone and provide connectivity to the other nodes in the network through multi hopping over the wireless links. As a natural extension to WLANs, the medium access mechanism of choice for these networks is the CSMA/CA based IEEE 802.11 distributed MAC protocol.

While IEEE 802.11 MAC protocol was designed for and provides a reasonable performance in a single hop network, it results in severe performance degradation in a multi-hop setting. In a single hop 802.11 network, all nodes contend for the channel with equal opportunity and act as greedy as possible to increase their one hop throughput which directly results in increase of the network aggregate throughput. In a multi-hop network, however, the greedy behavior of the nodes may result in service degradation as the packets transmitted by a source might not reach their final destination due to network congestion. In a congested network packets might be dropped in an intermediate node. Such a behavior will result in waste of the system resources used to deliver the packets to the intermediate node.

A congestion control scheme insures that the nodes place only as many packets on the wireless channel as can be delivered to the final destination. End-to-end schemes like TCP are the preferred solution in the Internet due to their scalability characteristics. In a wireless mesh network, however, a hop-by-hop congestion control scheme can be more appropriate as such a network does not have the scalability problems of the large-scale Internet. A layer 2 hop-by-hop solution reacts more quickly to congestion and is effective regardless of the traffic type.

The idea of Ad Hoc Networking is gaining popularity with the recent proliferation of mobile computers like laptops and palmtops. Minimal configuration, absence of infrastructure and quick deployment make Ad Hoc Networks convenient for emergency operations. Since host mobility causes frequent and unpredictable topological changes, the formation and maintenance of Ad Hoc Network is not only a challenging task and also it is different from the wired networks.

Ad Hoc Routing Protocols are classified into Proactive and Reactive type. Proactive routing protocols use the periodic update of information to know about the current topology while the reactive routing protocols create a route to a destination on demand basis. Few of the proactive protocols are DSDV [5], WRP [6], DBF [7] etc. while DSR [8], AODV [9], ABR [10] are few examples of reactive protocols. Even though no protocol is superior to the other, but the previous studies indicate that in general reactive protocols exhibit better performance than proactive protocols. [4]

This paper proposes a new algorithm to control congestion and security both in MANET by the use of queue threshold levels on each node along with a passphrase added on each node to involve the authentication based communication. For implementation NS2 simulator is being used with DSDV protocol for routing.

Rest of this paper is organized as follows:

Section II, describes the DSDV protocol along with various ADHOC networks. Section III, deals with proposed algorithm and section IV shows the results generated from simulations.

II. Existing System

A. Wireless Local Area Network (WLAN)

A wireless Local Area Network (WLAN) links two or more devices using some wireless distribution method (typically spread-spectrum or OFDM radio), and usually providing a connection through an access point to the wider internet. This gives users the mobility to move around within a local coverage area and still be connected to the network.

A wireless LAN is based on a cellular architecture where the system is subdivided into cells, where each cell (called Base Service Set or BSS*) is controlled by a Base station (called Access point or AP).

B. Wireless Mesh Network (WMN)

WMNs, generally described, consist of two types of nodes: mesh routers and mesh clients. The difference between a conventional router and a mesh router, apart from the mesh functionality, is that the latter can achieve the same coverage with lower transmission power through multi-hop communications. As regards to mesh clients, they also have necessary mesh functions and can thus behave as a router. On the other hand, gateway or bridge functions do not exist in these nodes. Additionally, mesh clients have only one wireless interface.

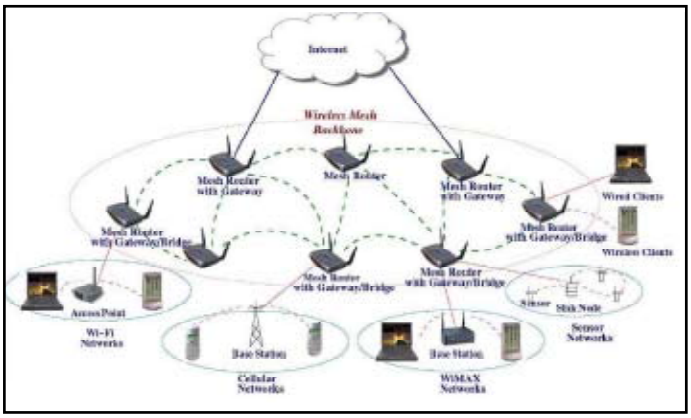

Fig. 1: Infrastructure/Backbone WMNs

III. Coordination Functions

A. Distributed Coordination Function (DCF)

The basic 802.11 MAC layer uses the distributed coordination function (DCF) to share the medium between multiple stations. DCF relies on CSMA/CA and optional 802.11 RTS/CTS to share the medium between stations. This has several limitations:

If many stations attempt to communicate at the same time, many collisions will occur which will lower the available bandwidth and possibly lead to congestive collapse.

There are no Quality of Service (QoS) guarantees. In particular, there is no notion of high or low priority traffic.

B. Point Coordination Function (PCF)

The original 802.11 MAC defines another coordination function called the point coordination function (PCF). This is available only in "infrastructure" mode, where stations are connected to the network through an Access Point (AP). This mode is optional and only very few APs or Wi-Fi adapters actually implement it. [Citation needed] APs send beacon frames at regular intervals (usually every 0.1 second). Between these beacon frames, PCF defines two periods: the Contention Free Period (CFP) and the Contention Period (CP). In the CP, DCF is used. In the CFP, the AP sends Contention-Free-Poll (CF-Poll) packets to each station, one at a time, to give them the right to send a packet. The AP is the coordinator. Although this allows for a better management of QoS, PCF does not define classes of traffic as is common with other QoS systems (e.g. 802.1p and DiffServ).

IV. Congestion Control

Although IEEE 802.11 Wireless Mesh Networks (WMNs) provide low-cost extension of wireless Internet access coverage, the wide adoption of WMNs is limited due to the bandwidth scarcity. One of the important mechanisms to fully utilize the scarce bandwidth is congestion control. Especially, congestion detection, a module of congestion control, plays an essential role since the source rates should be adapted according to the detected network congestion. Due to the various dynamics of IEEE 802.11 WMNs, wireless congestion control mechanisms usually use complicated combination of various metrics, such as channel-idle time, interface queue length and average link layer retransmission in intermediate nodes. However, this metric combination requires the sophisticated design of congestion control mechanism and eventually leads to the optimization difficulty. Thus, we propose a simple-yet-effective congestion detection metric, CORE (COngestion Residual timE). CORE measures the expected time of congestion-loss occurrence on the interface queue between IP and MAC layers. We obtain CORE by measuring the residual queue length and the slope of the queue length and then refining them with signal processing schemes (e.g., triangular moving average and linear regression).

Moreover CORE provides over-generated rate information that is essential to the congestion control mechanisms. By taking a series of experiments, we verify that CORE accurately predicts the time of congestion-loss occurrence as well as the over-generated rate.

V. Proposed Algorithm

The algorithm specified in base paper suffers with the following problems:

- Extra Overheads
- Works for High Density Network Topology

To reduce these problems, this work proposes to modify the IEEE 802.11 DCF Acknowledgement packet header to incorporate a new variable reliability and sender address to it, which shows the reliability of the node which is forwarding the acknowledgement. The whole work is as follows:

A. Model

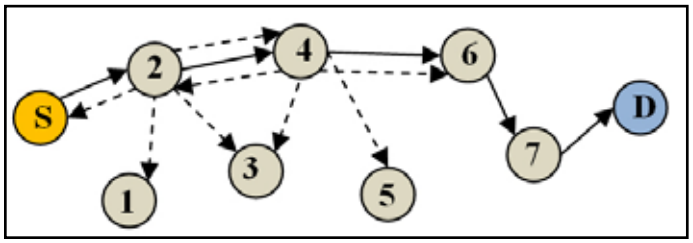

Fig. 2: Route from Source to Destination

B. Misbehavior Detection Mechanism

Bytes	2	2	6	6	6	4
	F.C.	Duration	RA	RL	SA	CRC

Fig. 3: Modified Acknowledgement Packet for IEEE 802.11 DCF

IEEE 802.11 DCF header is being modified to include a new field i.e. RL (reliability) of the ACK forwarder node and SA which is the address of the Sender Node. Here the thick lines shows the actual route decided by the sender node S to destination D and dotted arrows shows the acknowledgements to be given by the node to its neighbors.

In fig. 2, S sends the packet to node 2, by assuming that the RL value of every node is initially 0. Node 2 will forward the packet

to its successor node that is node 4. When node 4 will send an acknowledgement back to Node 2, its RL will be increased by one as the SA and address of the predecessor node will be matched, resulting in high RL value indicating that the node is reliable for future communication. All neighboring nodes (3, 5, and 6) will also overhear the acknowledgement but their RL will not be increased as their addresses will not match with SA field of the ACK header.

If node 4 is a misbehavior node, then will drop all the packets incoming to it after sending the acknowledgement to its predecessor node i.e. node 2. It will not be received by its successor node 6 and therefore it will not send the ACK to its predecessor. This will not allow increasing the RL value and hence the reliability of the node 4 is less causing it to be eliminated from the network.

C. Reports

Each node will be having the RL value which they will share with the neighboring nodes during the neighbor detection process. The RL value shall be used by any sender node to decide the route for communication with the destination.

1. Use of RL

It is to decide the reliability of the nodes which in turn will be used by the sender nodes to decide the route to the destination

2. Use of SA

It is the address of the sender, which will be used to increase the value of the RL when the receiver node will send the acknowledgement to the sender.

VII. Results & Discussion

All Existing work focused on one of the techniques either congestion control or security issues in MANET. This work proposes dynamically detecting packet dropper nodes and eliminated them by regarding them during the packet transfer on the basis of the reliability evaluated for each node. The algorithm applies the concept of reliability checking during each communication therefore the chances of dropper node elimination are very high. The processing is involved on each specific node therefore the traffic load is negligible during the application of the proposed algorithm.

VIII. Results

Each node will be having the RL value which they will share with the neighboring nodes during the neighbor detection process. The RL value shall be used by any sender node to decide the route for communication with the destination.

A. Use of RL

It is to decide the reliability of the nodes which in turn will be used by the sender nodes to decide the route to the destination

B. Use of SA

It is the address of the sender, which will be used to increase the value of the RL when the receiver node will send the acknowledgement to the sender.

References

[1] ZHANG Li, ZOU Jin,"A Wireless Ad Hoc Network Congestion Control Algorithm based on Game Theory", IEEE 978-0-7695-4422-9/11 International Conference on Future Computer Sciences and Application, 2011.

[2] Iftikhar Ahmad, Mata ur Rehman,"Efficient AODV routing based on traffic load and mobility of node in MANET", 978-1-4244-8058-6/10 IEEE 6th International Conference on Emerging Technologies (ICET), 2010.

[3] S. Corson, J. Macker,"Mobile Ad-Hoc Networking (MANET): Routing Protocol Performance issues and Evaluation Considerations", Network Working Group, RFC2501, January 1999.

[4] Khaleel Ur Rahman Khan, A Venugopal Reddy, Rafi U Zaman, K. Aditya Reddy, T Sri Harsha,"An Efficient DSDV Routing Protocol for Wireless Mobile Ad Hoc Networks and its Performance Comparison", IEEE 978-0-7695-3325-4/08, Second UKSIM European Symposium on Computer Modeling and Simulation, 2008

[5] C.E. Perkins, P. Bhagwat,"Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers", Computer Communication Review, 24(4), 1994, pp. 234-244.

[6] S. Murthy, J.J Garcia-Luna-Aceves,"An efficient routing protocol for wireless networks", ACM Mobile Networks and Application Journal, Special issue on Routing in Mobile Communication Networks, 1996.

[7] D. Bertsekas, Gallager, Data Network, pp. 404-410, second ed. Prentice Hall, Inc., 1992.

[8] David B. Johnson, David A. Maltz.,"Dynamic source routing in ad hoc wireless networks", Mobile Computing, Kluwer Academic Publishers, edited by Tomasz Imielinski and Hank Korth, chapter 5, pp. 153–181, 1996.

[9] C.E. Perkins, E.M. Royer,"Ad-Hoc on-Demand Distance Vector Routing", Proc. Workshop Mobile Computing Systems and Applications (WMCSA '99), Feb. 1999, pp. 90-100.

[10] C.K Toh,"Long-lived ad hoc routing based on the concept of associativity", Internet draft, IETF, March 1999.

I am Reeta Bourasi. I have done BE from Jabalpur Engineering Collage in 2006. I am pursuing M.Tech. from Sri Ram Institute of Technology, Jabalpur. I have been working as a lecturer in Computer Science Department in Khalsa Engineering College, Jabalpur since 2006 to till date. My subjects were network technology based and I have a good command on Operating System, Computer Graphics and ASP .net. I have good interpersonal skills and attitude to learn new things.