ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 2, May 2013

# DETECTION AND REMOVAL OF PACKET DROPPER NODES FOR CONGESTION CONTROL OVER THE MANET

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

Student, SRIT[1], Head of Department, M.Tech SRIT[2]

**Abstract**: - Packet Dropper nodes is a severe problem in MANET and they not only are harmful for the sender and receiver but they also lead to congestion in mobile adhoc networks as the sender may get involved in sending packets again and again as there is no acknowledgement from the receiver. Mobile ad hoc network is wireless network of mobile nodes, with no centralized management and control. Network congestion leads to reduced throughput, routing and lifespan, etc. of a network. Situation is worst when packet dropper nodes will send an acknowledgement to the sender and never forwards the packet ahead. Therefore they require proper attention and elimination from the network. In this paper, a new technique is being proposed to reduce the packet dropping nodes from the network by using a reliability factory which is increased on acknowledgement received from the receiver and all sender making decision to send a packet through a node having higher reliability factory. For calculating throughput, 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: ①the intrinsic properties of wireless multiple-hop links; ②the time varying of network topology; ③dynamic 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.

Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet.

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[8].

ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 2, May 2013

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 [4][10], WRP [5][13], DBF [23] etc. while DSR [9], AODV [6][15], 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.

## II. EXISTING SYSTEM

### Wireless local area network (WLAN)

The increased demands for mobility and flexibility in our daily life are demand that lead the development from wired LANs to wireless LANs (WLANs). Today a wired LAN can offer users high bit rates to meet the requirements of bandwidth consuming services like video conferences, streaming video etc. With this in mind a user of a WLAN will have high demands on the system and will not accept too much degradation in performance to achieve mobility and flexibility. This will in turn put high demands on the design of WLANs of the future.

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)[7].

## III. COORDINATION FUNCTIONS

### 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.

### 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).

ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 2, May 2013

## IV. CONGESTION CONTROL

MANET has been accepted as a communication medium in every field of the human life and applications areas of MANET are growing very fast. Acceptability of the MANET is imposing several severe requirements on MANET such as congestion control and security. In this work, the performance of DSDV (Destination Sequence Distance Vector) Routing protocol has been improved by providing an algorithm which is based on the pre decisions related with the congestion in the network. Inclusion of reliability factor makes it possible to detect the packet dropper nodes. This is not only improving the performance but also increasing the throughput of the network [3].

At Layer 2, congestion occurs as the MAC queue of an intermediate node in a multi-hop flow builds up. A queue buildup happens when a node is not able to forward traffic with a rate at least equal to the packet arrival rate. Whether congestion happens in the network depends on many different factors including network topology, channel capacity, number of flows and their paths, as well as the traffic characteristics. Figure 1 illustrates two example scenarios that can result in congestion in a throughput-fair system. In scenario (A), assuming the link capacities of all the three links are equal, the queue of Node C will build up as it gets an equal opportunity for transmission as either nodes A or B, and hence won't be able to forward all its incoming traffic. In scenario (B) similar situation occurs for Node B, where it needs to use its transmission opportunity to transmit traffic of flow f2 as well as to forward the traffic of flow f1 [3]. Regardless of its cause, congestion in a network results in waste of the resources that have been used to transfer the packets half way on their path and not to their final destination. If the resources that are used to transmit the packets which end up in the queue of a congested node and eventually get dropped are used more efficiently in the network, the overall system performance can be greatly improved.

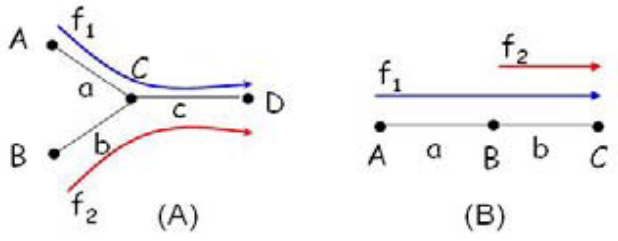



Figure 1: scenarios where congestion occurs.

## PROPOSED PROBLEM STATEMENT

Free-riding by packet dropping is one of the most important issues for the establishment and survivability of the open multi-hop wireless networks. In this paper, we focus on the data packet dropping in a rather dense Mobile Ad-hoc Network. To encounter this situation, we propose a scheme based on using MAC-layer acknowledgements to detect and punish packet dropper nodes. We used simulation-based results to evaluate the performance of our scheme. All simulations have been performed using NS2.

In a self-organized network, nodes are autonomous; they may free ride and may not cooperate properly in network operations to save their resources. Such nodes are called selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior. In this paper, we consider a rather dense self-organized MANET with a variable percentage of misbehaving nodes that attempt to free ride by dropping the data packets they should forward. Data packet dropping not only affects the network connectivity, but also can widely waste the network resources such as battery power of network nodes and available bandwidth of network links.

Our approach can be categorized as a Detection and Punishment-based approach. We use overhearing of MAC layer acknowledgments1 as a novel detection tool to detect misbehaving data packet-dropper nodes; so, in our system, such misbehaving nodes can be isolated from the network using the common reputation systems as used in previous methods. Since we describe and analyze our technique as an add-on for Dynamic Source Routing (DSR) protocol [9], the main idea of our detection system is as follows; when a forwarder node on a source route sends back a MAC-layer ACK for a received data packet that should forward it, this Acknowledgement (ACK) packet can both be received by the transmitter of related data packet and be overheard by all nodes in the transmission range of both ACK-transmitter and its successor node on the source route.

We call such ACK-transmitters and MAC-layer ACK packets, which will be sent back for a packet to be forwarded, observed node (ON), and forwarding-ACK respectively. We also call overhearing nodes as observer nodes and their behavior as observation.

Therefore, when an observer node overhears a forwarding-ACK packet, it will log this ACK and wait for another ACK packet; this time, from ON's successor node. If no ACK is overheard from successor node after sometime, it means that ON has not forwarded the received data packet to its successor node successfully. Then, this misbehaviour will be observed and reported to ON's predecessor node by the observer nodes. Predecessor node will collect, filter, and combine these reports to calculate the deviation of the behavior of its next node on the source route.

If its calculated deviation is greater than some value, it will send back a report to the source of the route. With the receipt

ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 2, May 2013

of this misbehavior report, source node will look for another route, containing no misbehaving node, to send its packets toward the destination node.

The title of my dissertation is: Detection and Removal of Packet Dropper Nodes for Congestion Control over the MANET.

- The topic is mainly oriented to provide congestion control over MANET.
- MANET has problems with the nodes which receive the packet and drop them in place of forwarding them towards destination.
- Such nodes causes problem of non reliable communication and may cause other network nodes to forward packets again and again causing unnecessary bandwidth utilization
- These also cause the wastage of battery of the other network nodes as they keep involved in sending packets towards the destinations

The proposed work concentrates detecting such packet dropper nodes and eliminating them from communication in future.

## NETWORK SIMULATOR

NS-2 is an Object-Oriented, discrete event network Simulator developed at UC Berkeley. It is written in C++ and OTcl (Object-Oriented Tcl) and primarily uses OTcl as Command and Configuration Language. NS is mainly used for simulating local and wide area networks. It simulates a wide variety of IP networks.

It implements network protocols such as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP), traffic source behavior such as File Transfer Protocol (FTP), Telnet, Web, Constant Bit Rate (CBR) & Variable Bit Rate (VBR), router queue management mechanisms such as Drop Tail, Random early detection (RED) and Collision Resolution Queue (CBQ), routing algorithms such as Dijkstra and more. NS also implements multicasting and some of the MAC layer protocols for LAN simulations. The NS project is now part of the VINT project that develops tools for Simulation results display, analysis & converters that convert n/w topologies generated by well-known generators to NS formats.

As shown in Figure 2, in a simplified user's view, NS is Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries (actually, plumbing modules are implemented as member functions of the base simulator object).

## OVERVIEW

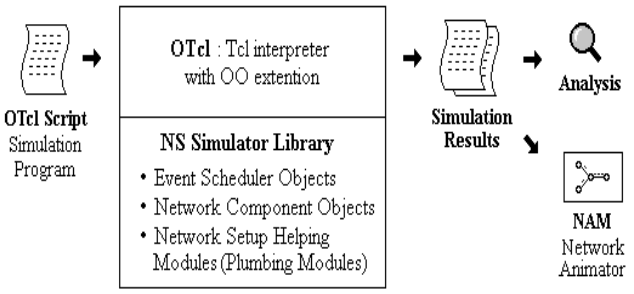



Figure 2 - NS-2 OVERVIEW

In other words, to use NS, programming in OTcl script language is required. To setup and run a simulation network, a user should write an OTcl script that initiates an event scheduler, sets up the network topology using the network objects and the plumbing functions in the library, and tells traffic sources when to start and stop transmitting packets through the event scheduler. The term "plumbing" is used for a network setup, because setting up a network is plumbing possible data paths among network objects by setting the "neighbor" pointer of an object to the address of an appropriate object. When a user wants to make a new network object, he or she can easily make an object either by writing a new object or by making a compound object from the object library, and plumb the data path through the object. This may sound like complicated job, but the plumbing OTcl modules actually make the job very easy. The power of NS comes from this plumbing.

## SIMULATION SCENARIO

TOOL USED FOR SIMULATION

Network Simulator (Version 2.32)

PARAMETERS

| | | |
|---|---|---|
| Bandwidth | – | 100 Mbps |
| Link Delay | – | 10 ms Drop Tail |
| Traffic Generator | – | CBR |
| Queue Size | – | 50 |
| Simulated for packet sizes | – | 128, 256, 512 bytes. |
| No. of Mobile Nodes created | – | 2,5,10,15,20,25,30,35 ,40, 50 |
| Simulation Time | – | 10 sec |

Table: Parameters use for creating network topology

ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 2, May 2013

PROGRAMMING

Files Modified

\ns-allinone-2.32\ns-2.32\mac\mac-802_11e.h
\ns-allinone-2.32\ns-2.32\mac\mac-802_11e.cc
\ns-allinone-2.32\ns-2.32\dsdv\dsdv.cc
\ns-allinone-2.32\ns-2.32\dsdv\dsdv.h
\ns-allinone-2.32\ns-2.32\dsdv\route.cc
\ns-allinone-2.32\ns-2.32\dsdv\route.cc

## 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:

**Model**

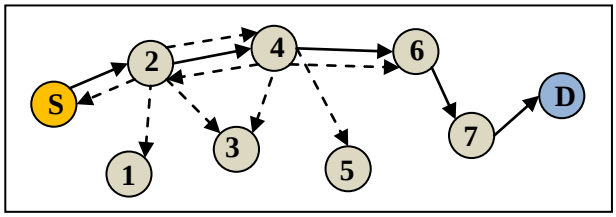



Figure 3: Route from Source to Destination

Misbehavior Detection Mechanism

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

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 figure 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.

**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.

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

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.

ISSN 2321 – 2004

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING
Vol. 1, Issue 2, May 2013

## 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.

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

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.

The reading and graphs drawn from results of the simulation done using NS2 simulator for variable number of nodes and different packet sizes (128, 256 and 512 Bytes) are as follows. The results has been processed first without modification of the files in NS2 and then with the modification done according to the proposed algorithms. The plots of the graphs are as under:

## NAM Result

As described above in discussion related with tools, NAM has been used to show the animation and working of the nodes. NAM draws the topology and nodes in it, which send and receive data packets over the network. Snap shot of the proposed *implementation is as follows:*

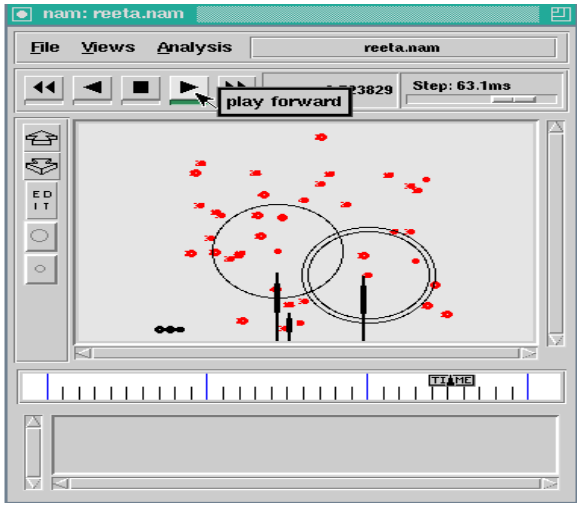



Figure 4: NAM Result screen showing animation over the network of 40 nodes

*The above show the NAM animation of the proposed work. In the figure black circle show the broadcast being performed by the nodes to the neighbours and the packet drops done by three nodes. The complete animation reveals that the packet drop is slowly elimination resulting in smooth communication. The animation behavior is indicative of the success of the proposed work.*

### *1) For Packet Size 128 Bytes*

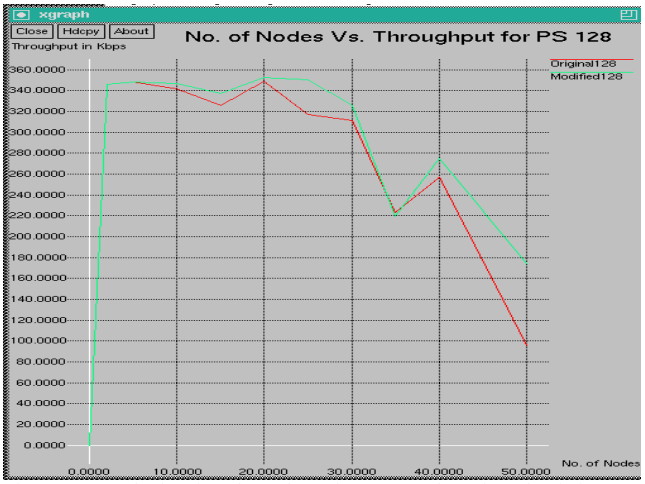



Figure 5: Graph showing throughput for proposed work and existing work with packet size 128 bytes

ISSN 2321 – 2004

IJIREEICE

*INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN ELECTRICAL, ELECTRONICS, INSTRUMENTATION AND CONTROL ENGINEERING*
*Vol. 1, Issue 2, May 2013*

**Inference:** The above graph and readings show that for the packet sizes of 128 bytes, the proposed work is having better throughput in all situations whether the number of nodes is less or more i.e. for the network of any density the proposed work performs better. In cases when the difference in throughput is having bigger difference, the network nodes are expected to be positioned nearby each other.

2) For Packet Size 256 Bytes

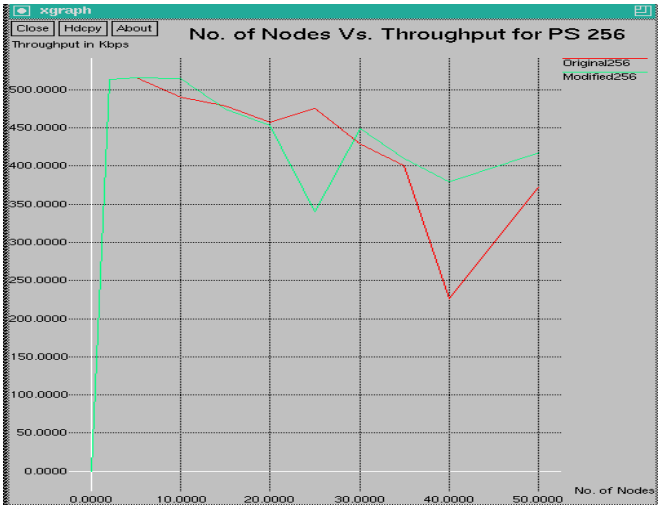


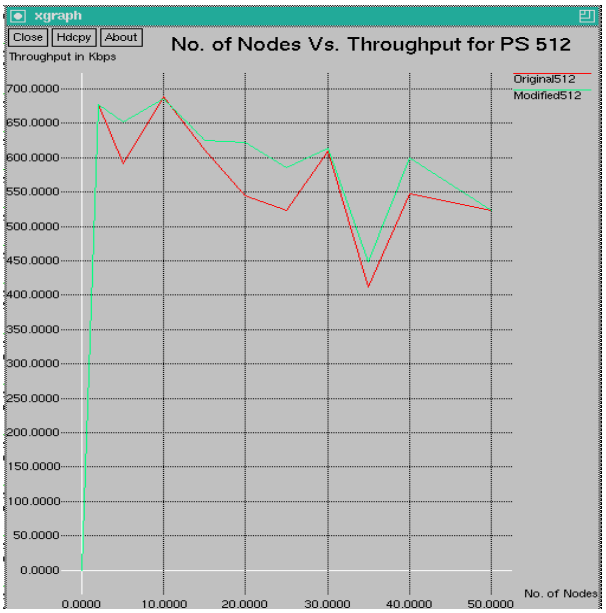

Figure 6: Graph showing throughput for proposed work and existing work with packet size 256 bytes

| Number of Nodes | Existing | Modified |
|---|---|---|
| 2 | 513.69 | 513.88 |
| 5 | 515.44 | 515.41 |
| 10 | 490.36 | 515.00 |
| 15 | 478.86 | 474.53 |
| 20 | 457.85 | 453.02 |
| 25 | 476.14 | 339.92 |
| 30 | 428.64 | 449.07 |
| 35 | 400.50 | 409.95 |
| 40 | 225.55 | 379.31 |
| 50 | 372.21 | 417.43 |

**Inference**: In the above case when packet size is 256 bytes, it is being found form the graphs and readings that there is a sharp decrease in throughput in comparison with the existing algorithm for the moderate density of network nodes. The expected outcome is not being matched mainly due the position of the nodes very far from each other causing the probability of loss of packets are higher. The proposed implementation shows good results otherwise as in case of packets of 128 bytes.

| ***Number of Nodes*** | ***Existing*** | ***Modified*** |
|---|---|---|
| 2 | 345.68 | 345.66 |
| 5 | 348.09 | 348.03 |
| 10 | 341.95 | 346.80 |
| 15 | 325.83 | 337.17 |
| 20 | 348.64 | 352.26 |
| 25 | 317.20 | 350.18 |
| 30 | 310.97 | 325.85 |
| 35 | 223.41 | 219.41 |
| 40 | 256.85 | 274.97 |
| 50 | 96.05 | 173.82 |

3) For Packet Size 512 Bytes




Graph showing throughput for proposed work and existing work with packet size 512 bytes

| **Number of Nodes** | **Existing** | **Modified** |
|---|---|---|
| 2 | 677.75 | 677.86 |
| 5 | 591.19 | 652.25 |
| 10 | 688.29 | 685.66 |
| 15 | 611.14 | 625.36 |
| 20 | 544.72 | 622.20 |
| 25 | 523.90 | 586.02 |
| 30 | 609.59 | 613.63 |
| 35 | 411.28 | 448.88 |
| 40 | 547.90 | 599.82 |
| 50 | 523.37 | 523.44 |

**Inference:** The above results indicate that the proposed work provides higher throughput even when the packet size is 512 bytes which proves that betterments achieved due to application of reliability mechanism proposed in this work.

Comparison with Base Paper:-

The algorithm proposed in the base paper is applicable when numbers of nodes in the network are too many i.e. for high density networks, which is not a feasible condition always, in this proposed work, network density can be as low as 2 nodes and still the results are better than working of DSDV protocol.The amount of work done for implementation of the proposed solution in base paper, results in high usage of the node energy even when the nodes are not dropping packets, whereas in this work the overall work done for communication will not use lot of energy of the individual nodes and hence the nodes will have higher working time period. The amount of work done for implementation of the proposed solution in base paper, results in high usage of the node energy even when the nodes are not dropping packets, whereas in this work the overall work done for communication will not use lot of energy of the individual nodes and hence the nodes will have higher working time period.

## VIII. CONCLUSION

From the above results and discussion it is clear that the proposed work is providing better performance in the case of all the packet size in respect of the existing NS2 protocol implementation for Wireless networks. From the graphs it is seen that there is sudden fall in throughput when network is increased to around 40 nodes. But similar fall of throughput in the existing protocol implementation indicates that this is not unusual behavior.

It is also concluded from the results drawn above that proposed work is providing similar high performance for both high density and low density networks.

## X. FUTURE WORK

The implemented work has been tested for density upto 50 nodes and it can be tested for high density of nodes having bigger mix of wired nodes and wireless nodes. The high density networks shall cause the high values of reliability and having nodes with almost equal reliability value will increase the competition among the nodes.

In future, this work can also be enhanced to test on other protocols such as AODV or DSR. The mechanism can also be tested for other output parameters such as end to end delay, packet delivery ratio etc.

## REFERENCES

1. Mehdi Keshavarz "MAC-Aided Packet-Dropper Detection in Multi-Hop Wireless Networks," Computer Eng. Department Islamic Azad University Qazvin, IRAN, 2012
2. Wireless Data Networking Standards Support Report: 802.11 Wireless Networking Standards, Oct 1, 2002
3. S. Corson and J. Macker, "Mobile AdHoc 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. Y. Su and T. Gross, "WXCP: Explicit congestion control for wireless multi-hop networks," in Proc. of IWQoS, Jun. 2005
6. Iftikhar Ahmad and 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
7. Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications, ANSI/IEEE Std 802.11, 1999
8. D. Qiao and K. G. Shin, "Achieving efficient channel utilization and weighted fairness for data communications in IEEE 802.11 WLAN under DCF," in Proc. of IEEE/IFIP International Conference of Quality of Service (IWQoS'02), May 2002
9. A.Kowshika, C.Maheswari, Dr.S.Karthik. "A Packet Forwarding Mechanism for MANET using MODRP in Dynamic Source Routing (DSR)," 2010 International Conference on Advances in Recent Technologies in Communication and Computing
10. ZHANG Li, ZOU Jin "A Wireless AdHoc Network Congestion Control Algorithm based on Game Theory," IEEE 978-0-7695-4422-9/11 International Conference on Future Computer Sciences and Application, 2011
11. C.E. Perkins & P. Bhagwat, "Highly Dynamic Destination Sequence-Vector Routing (DSDV) for Mobile Computers", Computer Communication Review, 24(4), 1994, 234-244.
12. Wireless Data Networking Standards Support Report: 802.11 Wireless Networking Standards, 2002
13. S.Murthy and 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
14. David B. Johnson and 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, pages 153–181, 1996
15. C.E. Perkins and E.M. Royer, "Ad-Hoc on-Demand Distance Vector Routing", Proc. Workshop Mobile Computing Systems and Applications (WMCSA '99), Feb. 1999, pages 90-100.
16. A. Warrier, S. Janakiraman, S. Ha, and I. Rhee, "DiffQ: Practical differential backlog congestion control for wireless networks," in Proc. of IEEE INFOCOM, Apr. 2009
17. V. A. Siris and C. Courcoubetis, "Resource Control for the Enhanced Distributed Channel Access (EDCA) Mechanism in IEEE 802.11e," FORTH-ICS, Tech. Rep. No. 352, March 2005, submitted for publication.
18. Hongqiang Zhai, Younggoo Kwon and Yuguang Fang "Performance analysis of IEEE 802.11 MAC protocols in wireless LANs", Sejong University, Seoul 143-747, Korea 2004
19. D. Qiao and K. G. Shin, "Achieving efficient channel utilization and weighted fairness for data communications in IEEE 802.11 WLAN under DCF," in Proc. of IEEE/IFIP International Conference of Quality of Service (IWQoS'02), May 2002
20. Hongxun Liu, Jose G. Delgado-Frias, " Using a cache Scheme to Detect Misbehaving Nodes in Mobile Ad-Hoc Networks," Electrical Engineering and Computer Science Washington State University Pullman ,WA 99164-2752,USA , 2007

21. Farooq Anjum, "Lightweight Packet Drop Detection for AdHoc Networks", Telcordia Technologies Piscataway, NJ 08854, 2004
22. Xu Li, Rongxing Lu, Xiaohui Liang, and Xuemin (Sherman) Shen "Side Channel Monitoring: Packet Drop Attack Detection in Wireless AdHoc Networks," Department of Electrical and Computer Engineering, Universiti of Waterloo, 2011

## BIOGRAPHY

**Sandeep Sahu**, I had done my Bachelor Of Engineering degree in computer science from a government institute (M.P.). Master of Technology in Computer Science & Engineering from Indian Institute of Technoly, Guwahati (Assam). My research areas are wireless sensor network, mobile adhoc network, wireless networks and cloud computing.

I am **Reeta Bourasi**, Working as Lecturer in Computer Science and Engineering department in Khalsa Engg. College, Jabalpur.