A NOVEL IMPLEMENTATION OF BACKPRESSURE ALGORITHM IN WIRELESS AD HOC NETWORK

[1]Ugendhar Addagatla,[2]Dr. V. Janaki
[1]Department of C.S.E, Guru Nanak Institutions Technical Campus, Ranga Reddy, Telangana-501506
[2]Department of C.S.E, Vaagdevi Engineering College, Warangal, Telangana-506005
ugendhar2009@gmail.com

ABSTRACT:- In the wireless networks, the routing process is the one of the major concern and it is the fundamental process in the ad hoc networks. To aid this exertion, we proposed an experimental assessment of backpressure mechanisms for wireless networks. By this proposed system, we will address many scheduling and routing problems and also improve the throughput and delay that are mainly caused by the packets at the node transmission.TheBackpressure routing is a compact and increased throughput for wireless networks, but undergoesincreased delays. In routing, the backpressure algorithm is known to afford throughput optimality with dynamic traffic. The important assumption in the backpressure algorithm is that all nodes are benevolent and observe the algorithm rules leading the information exchange and principal optimization requirements.In the proposed system, we demonstrate that how the node is stabilize at the backpressure algorithm routing and also by jointly alleviating the virtual trust queue and the real packet queue.The backpressure algorithm not only accomplishesflexibility, but also tolerates the throughput performance undersecurity attacks. This system is mainly enhances the node behavior at the time of communication and also it improves the node security at the time of many threats in the wireless applications.

KEYWORDS: -Backpressure Algorithm, throughputoptimality, dynamictraffic, node transmission

I. INTRODUCTION

Wireless ad hoc networks lack stationary infrastructure e.g., base stations. Due to this, the communication between any two nodes that are out of one another's transmission range is attained through intermediary nodes. These middle nodes relay messages to set up a communication channel. Modern applications of the ad hoc networks consistofbattle fields, disaster release, and accuracyin farming, e-health, and oceanobserving with submerged wireless sensor networks. In this type of networks, Packet broadcast scheduling is anessentialconcernas it is directly related to the success of a Quality of Service and a lowest use of system possessions. It is frequentlydignified in terms of the average packet delay, transmission rate and extreme delay, and the chief system source to be saved is the nodes' energy in order toextendnetworkgeneration. Besides delay and energy optimization, any packet routing algorithm for ad hoc networks must be robust to topology variations and attempt for throughput.As a result of the insufficiency of wireless bandwidth resources, it is important to proficientlyemploy resource to maintain high throughput, high-quality communications over wireless networks. In this setting, decent routing and planning algorithms are required to vigorouslyassign wireless resources to exhaust the possibilities the network throughput section. To report this throughput-optimal routing and planning has been expansively studied. However these algorithms exploit the network throughput region, further issues need to be deliberated for practical arrangement.

By means of the substantial increase of real-time traffic, end-to-end delay turns out to be very significant in network algorithm scheme. The customary back-pressure algorithm alleviates the network by manipulating all possible paths between source–destination pairs. Whereas this might be required in a severely loaded network, this appearsexcessive in a light or reasonable load system. Discovering all paths is in fact harmful; it leads to packets negotiating excessively long paths between sources and destinations, leading to large end-to-end packet delays. Backpressure algorithms have justestablished much consideration for mutually routing and scheduling over wireless networks. This project presents a routing/scheduling back-pressure algorithm that not only guarantees network stability (throughput optimality), but also adaptively selects a set of optimal routes based on shortest-path factsso as tolessen average path lengths between each nodes.

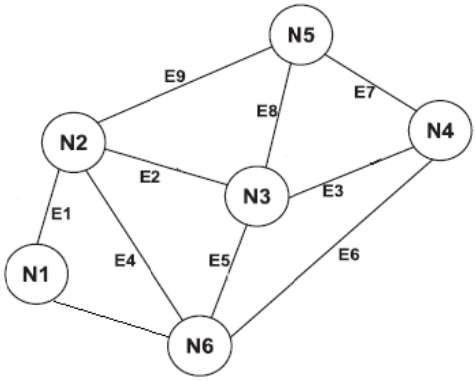

Fig.1: Example of a Wireless ad hoc network topology with six nodes

The performance of backpressure depreciates in situations of low, and moderate in the network, i.e., this algorithm alleviates the system using all possible paths all over the network. The adverse effect of this algorithm is to raisedelay and also to increase the energy consumption of the nodes. This is because of End to end delay and energy consumption isconsistent. The minimization of the average time that the packets stay in the systemsuggests a decrease in the average number of hops that the packs travel until they influence their destination, which in turn suggests a decrease in the totalenergy consumption.

II. BACK PRESSURE ROUTING

Backpressure routing denotes to an algorithm for routing traffic over a multi-hop network by using jamminggrades. This algorithm can be applied to wireless networks, comprising sensor networks, mobile ad-hoc networks, and various networks with wireless and wire line constituents. Backpressure techniques can also be applied to other parts, such as to the study of product association systems and treating networks. This proposed system concentrates on communication networks, where packets from multiple data torrentsreach and must be distributed to suitable destinations. The backpressure algorithm activates in located time, and every slot it pursues to route data in commands that maximize the distinction backlog between neighboring nodes. In core, the backpressure algorithm organizes transmissions and exploits the amount of total data delivery by familiarizing scheduling and routing assessments based on each node's per-flow queue bottlenecks and channel rates when smeared to wireless networks. To this end, it believes that all nodes follow the algorithm rules of information exchange, ideal link stimulation, and flow assortment. Nevertheless, in practice, a node may intentionallydisturb any rule to break the fundamentalevidenceexpected by the backpressure algorithm. Irrespective of its selfish or malevolentdetermination, there are two basic ways for an aggressor to follow: it can misrepresent any information used in the backpressure algorithm and it can interrupt backpressure algorithm based protocols by contributing no cooperation and/or not resulting decisions in routing and planning optimization. These possible attacks pose a major hurdle to real deployment of the backpressure algorithm in real systems.

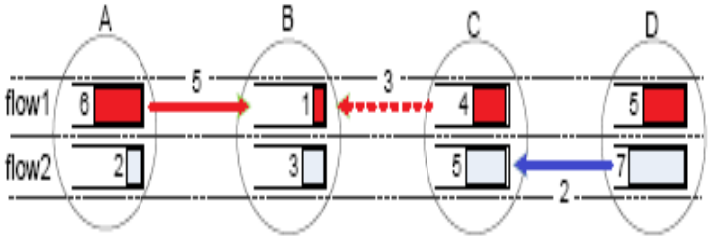

Fig.2. An example of backpressure algorithm

The above figure demonstrates the working principle of backpressure algorithm. In this setup, Nodes A, B, C, and D form a three hop wireless network with two flows. Each node has the same transmission rate and cannot transmit and receive at the same time slot. At a specified time slot, the backlog of each node for each flow is demonstrated in Fig. 1. The backpressure algorithm works as follows.

i) Compute the maximum differential queue backlog between each node pair as a link weight; i.e., A→B is 5 for flow 1, C→B is 3 for flow 1, and D→C is 2 for flow 2, and select these three links.
ii) List all non-conflicting link sets, i.e., {A→B for flow 1, D→C for flow 2} and {C→B for flow 1}.
iii) Choose the set that maximizes the sum of all link weights, i.e., {A→B for flow 1, D→C for flow 2}.

III. PROPOSED SYSTEM

3.1. Backpressure Algorithm

The backpressure algorithm is the ideal solution that necessitatescentralorganization. In reality, aintegrated controller will gather information from all nodes then sort the planning decision. There also happen low-complexity, spreaded solutions with performance near to the best solution. The backpressure algorithm creates routing and scheduling decisions based on

$$\mathbf{u}^*(t) = \arg\max_{\mathbf{u}(t)\in\mathcal{R}(t)} \sum_{u_{i,j}(t)\in\mathbf{u}(t)} u_{i,j}(t) w_{i,j}(t), \quad \text{------(1)}$$

$$w_{i,j}(t) = \max_{f\in\mathcal{F}} \left(Q_i^f(t) - Q_j^f(t)\right), \quad \text{-------(2)}$$

Where,

u*i, j*(t) ϵ u(t) is the link rate from node i to j

u(t) is a feasible rate vector in the set of all feasible rate vectors

R(t) in the network

Wi,j(t) is the maximum differential queue backlog.

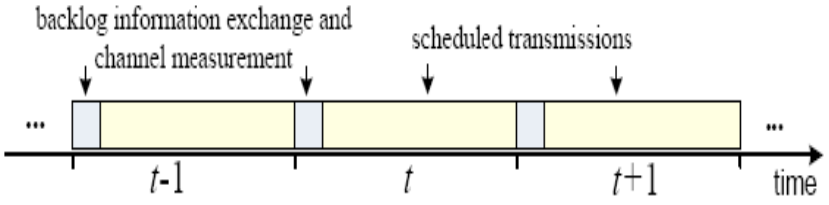

Fig.2. Information exchange and transmission scheduling in the backpressure algorithm

The fig.2 shows the generic operational model for the backpressure algorithm at the starting of each time slot; nodes send information to the director for centralized coordination. The information contains queue bottlenecks for computing the differential queue backlog wi,j(t) in (2) and network state information created on networkdimensions for attaining the best channel rate ui,j(t) from any node i to node j in (1). Formerly, planned transmissions arise at the rest of the time slot. The security solution is mainly based on the comprehensive optimization such as it does not need extra compacted or global information, but familiarizes new local information. Consequently, it can be readily stretched to disseminatedvarieties that rely on exchange of local statistics only. The backpressure algorithm is throughput-optimal and disappointscommunicating to blocked nodes, exploiting all possible paths between source and destination. This asset leads to redundant end-to-end delay when the traffic load is light. Furthermore, using extended paths in the situation of light or moderate traffic wastes network assets.

Algorithm 1: Backpressure at node i

for $t = 0, 1, 2, \cdots$ **do**
  Observe local queue lengths $\{q_i^k(t)\}_k$ for all flows k
  for *all neighbors* $j \in n_i$ **do**
    Send queue lengths $\{q_i^k(t)\}_k$ – Receive $\{q_j^k(t)\}_k$
    Determine flow with largest pressure:

$$k_{ij}^* = \underset{k}{\operatorname{argmax}} \left[q_i^k(t) - q_j^k(t)\right]^+$$

    Set routing variables to $r_{ij}^k(t) = 0$ for all $k \neq k_{ij}^*$ and

$$r_{ij}^{k_{ij}^*}(t) = C_{ij}\mathbb{I}\left\{q_i^{k_{ij}^*}(t) - q_j^{k_{ij}^*}(t) > 0\right\}$$

    Transmit $r_{ij}^{k_{ij}^*}(t)$ packets for flow k_{ij}^*
  end
end

3.2 Threats in Backpressure Algorithm

In common, the performance of an insider attacker can be categorized to one or both of the following two groups.

- Information-falsification attack: this occurs during the information altercationstage at the opening of each time slot, where the aggressorpurposefully sends false information to others to undesirably affect backpressure routing.As the backpressure algorithm is responsive to node queue bottlenecks and channel state information, its routing results can be suggestively affected by information-falsification attacks.
- Protocol-violation attack: this occurs in the arranged transmission stage, where the aggressor does not submit backpressure routing decisions.

3.3. Security actions in Backpressure Algorithm

The Backpressure Algorithm has resilient on several attacks .Suchattacks can ensure at least one of two objectives: (i) selfishbehavior: if the assailant is selfish, it is concerned in its ownbehavior gain without care for others in the network;(ii) malicious behavior: if the assailant is malicious, it intendstodestroy the throughput of others in the network.As the backpressure algorithm needs nodes to transmission their linebottlenecks and network state information, one operative way for an attacker to achieve its selfish or malevolent intent is to misrepresent its queue backlogs or network state information.

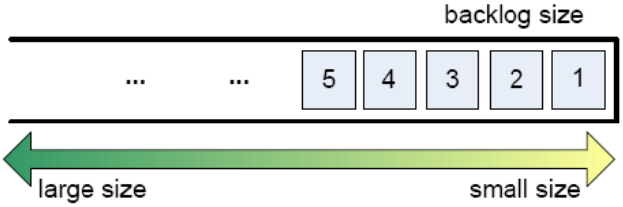

Fig.3:Large and small backlog size broadcasting can be used to disturb backpressure routing.

- **Manipulating backlogs:** If the invaderrequiressending its own packets instantaneouslyin place of receiving packets from others, it can broadcast counterfeit higher backlogs than actual ones.Finally, an attacker can operate its backlog information subjectively to distress the optimization solution in the backpressure algorithm.
- **Counterfeit channel state information**: If the aggressordesires to gain the transmission chance, it can broadcast higher channel gains than the tangibleones.While broadcasting false channel information is one type of information prevarication, we can classify attacks that forge channel state information into protocol-violation attacks. This is for the reason that when an attacker cannot communicate with a demanded rate, it disturbs the scheduling decision.

3.4 Virtual Trust Queue to Secure Backpressure Algorithm

The main aim is to design aapproach based on assessing packet arrival rates to protect the backpressure algorithm. We familiarize an amplified optimization method to defend the backpressure algorithm, and then existent how to build a widespread virtual trust queue solution to provide the safetyassurance.

There are three major shortcomings of this approach are

(i) if an attacker causes a very large value of Di,j(t) at time t (e.g., deliberately dropping all packets) and then returns to legitimate behavior after time t, the penalty only happens and lasts during time t (i.e., there is no memory in tracking the trust), and therefore may not mitigate the total damage of the attack;

(ii) There is no systematic way to determine the value of v; and

(iii) There is no methodical way to recognize, control, or limit the damage that an attacker can cause to the network behavior.

To deliberate the firstdispute, it is to define a glidingwindow to record the past and keep smearing the disadvantage. Nevertheless, the sliding window method necessitatescareful adjustment of window size and still cannot solve the second and third issues.The virtual trust queue mechanism is centered on the explanations on other nodes, which may have faults in the real world. Such faults may also make possible false allegation to some benevolent nodes.

IV. FALSIFYING VIRTUAL TRUST QUEUE INFORMATION

The virtual trust queue mechanism is mainly used to coordinate node transmissions. In one hand, virtual trust queues provide attackflexibility; in contrast, they may announce another line of susceptibility in the backpressure algorithm.Specifically, nodes wantto broadcast extra virtual trust queue information for either spreadorcentral coordination at time t. Nonetheless, it is possible that an aggressor can also fake virtual trust queue information to liability a genuine node for misconduct. Or even worse, two or more attackers can conspirewith each other to make an untraceablesetting, in which one attacker is offensive the network by operatinginformation or impious the protocol, and at the same time other attackers follow the schedule but send counterfeit trust queue information to protect for the attacker.

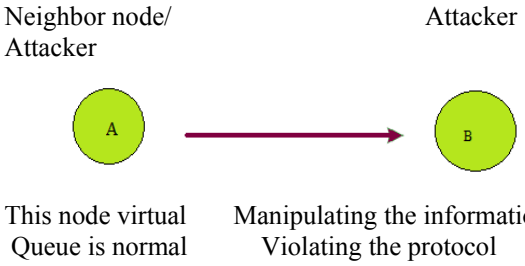

Fig.4. Two nodes can collude with each other.

The above figure demonstrates the Node A is aggressive the network and at the same time, its partner node B asserts that node A's virtual trust queue is normal.These attacks can be all understood via the same planof falsifying virtual trust queue information. Consequently,it is essential to address such attacks with an operativecountermeasure.The algorithm asymptotically elucidates the hop minimization problem as, but remunerates a price of progressively large backlogs in the network. On stochastic control of wireless networks comparable tuning restrictions have also been familiarized. Financial usage of energy is a precarious issue in Wireless Networks. Communication is the most energy affluent activity a node accomplishes. Energy necessary to transmit varies exponentially with transmission distance; consequently, it is expected to use multi-hop communication in WSNs. A WSN's life-time mostly depends on how professionally it transmits a data packet from its source to its destination.

For a central backpressure application, it is easy to let the controller to choose which nodes arefakingvirtual queue information. The projected trust mechanism can also be used in a completelydisseminatedsetting. On the other hand, aimportant issue is then who will gather such information and select which nodes is faking the virtual queue information. A usual way is to let every neighbor to connect with each other then decide separately who is falsifying the information. A malevolent neighbor may try to send or forward the forged information to other neighbors to affect their resolution.Finally,determine that the trust mechanism is less lenient of the number of malicious nodes in the distributed backpressure backgroundthan it is in the central one.

V. PERFORMANCE EVALUATION

In this performance evaluation, an extensive simulation study is to estimate the performance of the intended secure backpressure algorithm in a node. The setup of the wireless network includes 50 nodes with broadcasting range 80m consistentlyspread over specified area. The protocol interference model is adopted. Furthermore, if a node is receiving from a neighbor at a time slot, none of its other neighbors will be planned to transmit.Wedeliberate a complete set of attack situationsin the models:

- ✓ Black hole attacks is the attacks in which it continuously broadcast zero queue backlogs and high frequency rates to fascinate packets to be directed to them, then drop all received packets.
- ✓ On-off attacks in which perform as black holes or sincere nodes during on and off periods.

- ✓ Selfish nodes always challenge to empty its queues by propagating high queue backlogs to detention the transmission opportunity.
- ✓ Heterogeneous attacks include all above attackers at different nodes in the same network.

In the performance evaluation, we describe the metricof throughput as the average amount ofdistributed data per time slot normalized by the link rate.

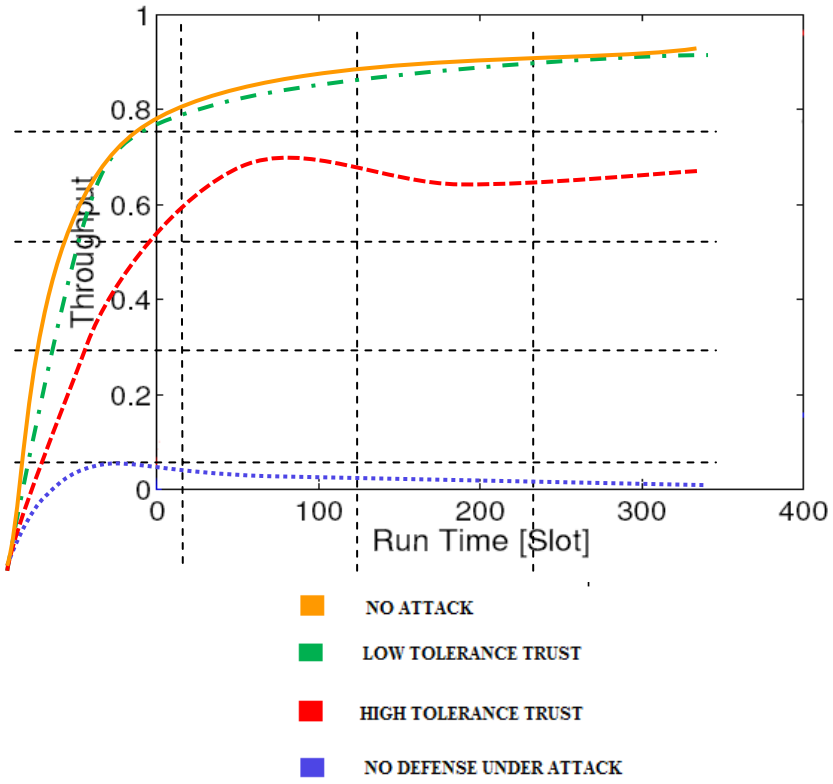

Fig.5: Throughput over run time for different scenarios

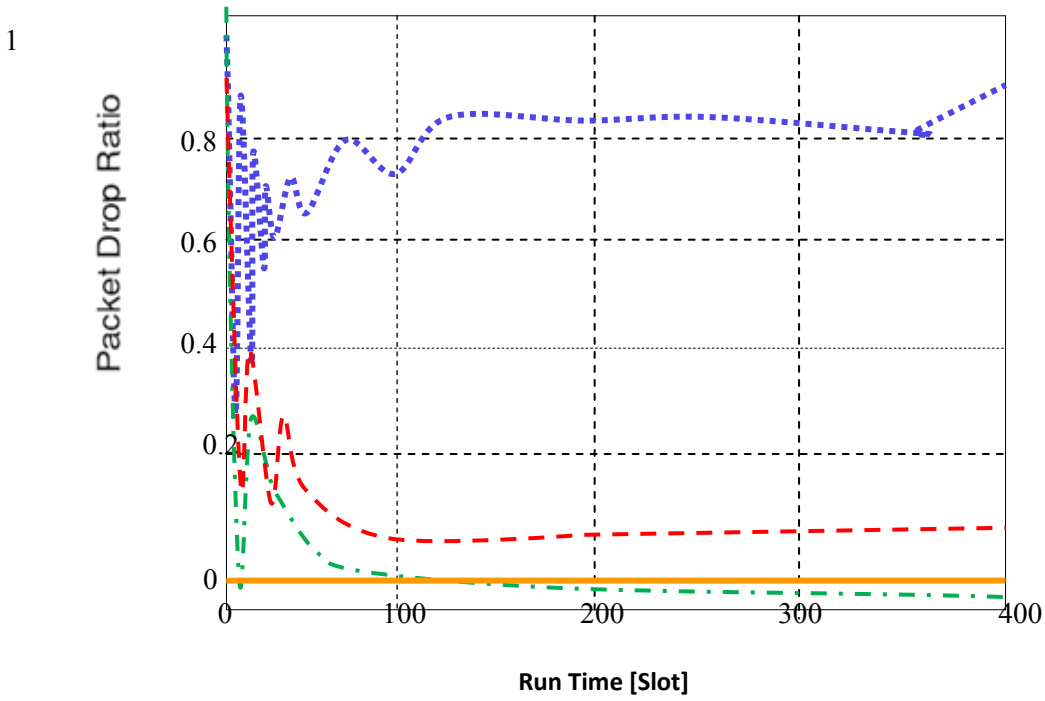

Fig.6: Packet drop ratio over run time for different scenarios

In simulation process, randomly select one node in the network performing as a blackhole. Fig.5demonstrates the throughput in the network under the blackhole attack.Initially, the network throughput rises as run time passes. This is because the network is casuallyburdened in the initial state. As additional packets reach at each node, the network throughput increases progressively and becomes constant. Though, when there is an attacker, we can see over 85% deprivation of the throughput in the network. The output of the system is mainly concentrates on the improving efficiency. If an attacker activatesoutside the given acceptance level,which results in an unstable queue, the attacker willbe excluded from the routing decision. Fig. 6illustrates the packet drop ratio in network under the same attacks. We observe from the figure, the packet drop ratio is zero lacking the attack. Hence, in the proposed system, throughput is increased and the packet drop ratio is decreased.

VI. CONCLUSION

In this proposed system, we provided anefficientworkon the backpressure algorithm at the node level and also enhance the security of the network. Lastly, weshowedcomprehensive simulations to authenticate the efficiency of the suggested mechanism. The results exhibited that the virtual trust queue mechanism acquires the backpressure algorithm in contradiction of a wide range of attacks. Consequently, the solution from this proposed systemdissipates a major barrier for practical arrangement of backpressure algorithm for protected wireless applications. Hence, the backpressure algorithm not only achieves flexibility, but also endures the throughput performance under security attacks. This system is generally improves the node behavior at the time of communication and also it progresses the node security at the time of many threats in the wireless applications.

REFERENCES

[1] Maglaras, L.A. and Katsaros, D. (2011) Layeredbackpressure scheduling for delay reduction in ad hoc networks. In World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2011 IEEE International Symposium on a (IEEE): 1-9.

[2] Gupta, G. and Shroff, N. (2009) Delay analysis for multi-hop wireless networks. In INFOCOM 2009, IEEE: 2356-2364.

[3] A. Warrier, S. Janakiraman, S. Ha, and I. Rhee, "DiffQ: Practicaldifferential backlog congestion control for wireless networks," inProc. of IEEE INFOCOM, 2009.

[4] F. Bao, I.-R. Chen, M. Chang, and J.-H Cho, "Hierarchical trust management for wireless sensor networks and its applications to trust-based routing and intrusion detection," IEEE Trans. Network and Service Management, vol. 9, pp. 169–183, Mar. 2012.

[5] L. Georgiadis, M. J. Neely, and L. Tassiulas,"Resource allocation and cross-layer control in wireless networks," Foundations and Trends in Networking, vol. 1, pp. 1–144, 2006.

[6] H. Seferoglu and E. Modiano, "Diff-Max: Separation of routingand scheduling in backpressure-based wireless networks," in Proc.of IEEE INFOCOM, 2013.

[7] S. Moeller, A. Sridharan, B.Krishnamachari, and O. Gnawali Routing without routes: The backpressure collection protocolProc. 9thACM/IEEE Intl. Conf. on Information Processing in Sensor Networks (IPSN), April 2010.

[8] L. Huang, S. Moeller, M. J. Neely, and B. Krishnamachari. LIFO-backpressure achieves near optimal utility-delay tradeoff. Proc. WiOpt, May 2011.

[9] L. Huang, S. Moeller, M. J. Neely, and B. Krishnamachari,"LIFO-backpressure achieves near optimal utility-delay tradeoff,"ACM/IEEE Trans. Networking, pp. 831–844, June 2013.

[10] L. Bui, R. Srikant, and A. L. Stolyar, "A novel architecture for delay reduction in the back-pressure scheduling algorithm," IEEE/ACM Trans. Netw., vol. 19, no. 6, pp. 1597–1609, Dec. 2011.

[11] M. Alresaini, M. Sathiamoorthy, B. Krishnamachari, and M. J. Neely,"Backpressure with adaptive redundancy (BWAR)," in Proc. of IEEE INFOCOM, 2012.

[12] J. Nunez-Martinez, J. Mangues-Bafalluy, and M. Portoles-Comeras, "Studying practical any-to-any backpressure routing inWi-Fi mesh networks from a Lyapunovoptimizationperspective,"inProc. of IEEE MASS, 2011.

[13] Bui, L., Srikant, R. and Stolyar, A. (2009) Novel architectures and algorithms for delay reduction in back- pressure scheduling and routing. In INFOCOM 2009, IEEE (IEEE): 2936-2940.

[14] B. Radunovic, C. Gkantsidis, D. Gunawardena, and P. Key. Horizon: Balancing TCP over multiple paths in wireless mesh networkACMMobicom, 2008.

[15] Ying, L., Srikant, R., Towsley, D. and Liu, S.(2011) Cluster-based back-pressure routing algorithm. Networking, IEEE/ACM Transactions on 19(6): 1773-1786.

[16] J.-Y. Yoo, C. Sengul, R. Merz, and J. Kim, "Experimental analysisof backpressure scheduling in IEEE 802.11 wireless meshnetworks," in Proc. of IEEE ICC, 2011.

[17] Li, R., Eryilmaz, A. and Li, B. (2013) Throughput optimal wireless scheduling with regulated inter-servicetimes. In INFOCOM, 2013 Proceedings IEEE: 2616-2624.

[18] L. Ying, S. Shakkottai, A. Reddy, and S. Liu,"Oncombiningshortest-path and back-pressure routing over multihopwirelessnetworks," IEEE/ACM Trans. Networking, vol. 19, Jun 2011.

[19] S. Liu, L. Ying, and R. Srikant,"Throughput-optimal opportunisticscheduling in the presence of flow-level dynamics," IEEE/ACMTrans. Networking, vol. 19, Aug 2011.

[20] L. Bui, R. Srikant, and A. L. Stolyar,"Optimal resource allocation for multicast flows in multihop wireless networks," Phil. Trans. Roy. Soc., Ser.A, vol. 366, pp. 2059–2074, 2008.

Author Profile

UgendharAddagatla presently working as Associate professor in the department of Computer Science and Engineering at Guru Nanak Institutions Technical Campus, Ibrahimpatnam, Hyderabad, Telangana State, INDIA. He has 12 years of teaching experience. He is associated with ISTE and CSI as life member. He has obtained B. Tech. degree in Computer Science and Engineering from ChristuJyothi Institute of Technology and Science, Warangal, Jawaharlal Nehru Technological University Hyderabad, in 2003, M.Tech. degree in Software Engineering from Ramappa Engineering College, Warangal, Jawaharlal Nehru Technological University Hyderabad, in 2008 and my area of Research interest is Mobile Computing, Ph.D (CSE) from Jawaharlal Nehru Technological University, Hyderabad and it is my part of Research work.

Dr. V. Janaki received Ph.D degree from J.N.T. University Hyderabad, India in 2009 and M.Tech degree from R.E.C Warangal, Andhra Pradesh, India in 1988. She is currently working as Head and Professor of CSE, Vaagdevi Engineering College, Warangal, India. She has been awarded Ph.D for her research work done on Hill Cipher. Her main research interest includes Network security, Mobile Adhoc Networks and Artificial Intelligence. She has been involved in the organization as a chief member for various conferences and workshops. She published more than 50 research papers in National and International journals and conferences. She is presently supervising nearly 10 scholars for their research.