# Increasing Throughput for Data Transmission Using Back Pressure Algorithm

D. Uma Maheswari
Assistant Professor in Computer Science Department, Vidhyasagar College of Arts and Science, Udumalpet, Tamil Nadu, India

S. Karthigai Veni
M.Phil Scholar, Vidhyasagar College of Arts and Science, Udumalpet, Tamil Nadu, India

**Abstract – Network is the most important factor for data transmission. While sending the data it faces many problems like packet loss, mismatch packets, loss of continuation of data, etc. These problems were occurred due to throughputs of the networks. Transferring of the data throughput is the most important factor for avoiding the lossless transmission. To avoid the throughput problem we have to increasing the network throughput. By increasing the throughput here we use the backpressure algorithm for avoiding lossless transfer of data. After increasing the throughput they were faces the security problem, for this issue here we used the trusted node of data transmission were used and also cryptographic method of key attribute based mechanism were used for secure level of data transmission. By using this approach it provides the secure data transmission.**

**Index Terms – WSN, Data Transmission, Increasing Throughput, Trusted Node and Security.**

## 1. INTRODUCTION

Wireless sensor network is an emerging field where lots of research work has been done involving hardware and system design, networking, security factor and distributed algorithm. Nodes use to send data packet locally to its single hop neighbor nodes and so on and finally it reaches to its base station. Initially nodes are deployed flying from aircrafts or randomly and some time node changes its initial position (the time of deployment) and moves across the region based on the requirement; so this type of nodes is called mobile nodes. So there are two types of data transmission in wireless sensor network, these are – direct transmission and multi-hop data transmission. In direct transmission data are send directly to the sink where as multi-hop transmission data send via no of intermediate nodes lies between source node and base station [1]. In sensor network the flow of data is very important aspect

because each data packet contains the event which may be very important for some application. Due to the scarcity of wireless bandwidth resources, it is important to efficiently utilize resources to support high throughput, high-quality communications over multi-hop wireless networks.

In this context, good routing and scheduling algorithms are needed to dynamically allocate wireless resources to maximize the network throughput region [2]. To address this, throughput - optimal routing and scheduling, first developed in the seminal work has for a comprehensive survey. While these algorithms be extensively studied. We refer to maximize the network throughput region, additional issues need to be considered for practical deployment. With the significant increase of real-time traffic, end-to-end delay becomes very important in network algorithm design.

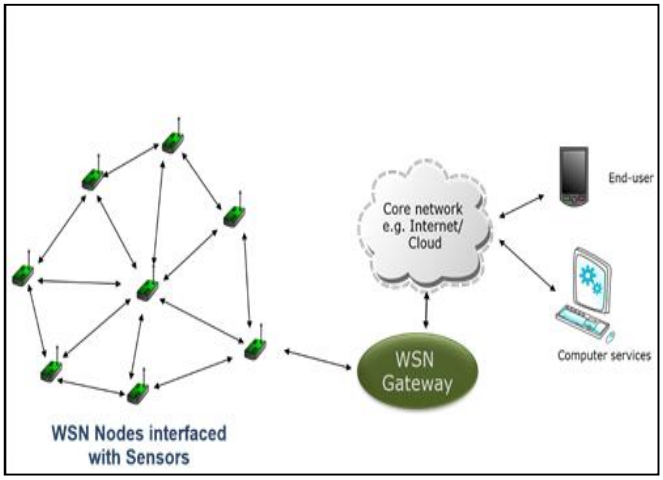


Figure 1: WSN Architecture

The traditional back-pressure algorithm stabilizes the network by exploiting all possible paths between source–destination pairs (thus load balancing over the entire network). While this might be needed in a heavily loaded network, this seems unnecessary in a light or moderate load regime [3]. Exploring all paths is in fact detrimental—it leads to packets traversing excessively long paths between sources and destinations, leading to large end-to-end packet delays. This paper proposes a new routing/scheduling back-pressure algorithm that minimizes the path lengths between sources and destinations while simultaneously being overall throughput-optimal. The proposed algorithm results in much smaller end-to-end packet

delay as compared to the traditional back-pressure algorithm. But sensor node has limited energy and limited memory capacity so maintaining security is difficult for them. It should be made sure that, the reports from the 'sensors in action' are authentic and reach the base station (BS) without any fabrication or modification [4]. The task of securing wireless sensor networks is however, complicated because sensors are highly anonymous devices with a limited energy and memory capacity, and initially they have no knowledge of their locations in the deployment environment. To make the data transmission secure some basic aspects of security has to be maintained during transmission. Here we discussed how the authentication and confidentiality maintained during data transmission because without this two parameter data transmission cannot be reliable; also we discussed how the missing packets can be detected during transmission by some efficient methods. In this paper we will discuss various ways to make the data transmission secure and efficient; also we will discuss some mechanism and protocol used in secure data transmission. In essence, the backpressure algorithm coordinates transmissions and maximizes the amount of total data delivery by adapting scheduling and routing decisions based on each node's per-flow queue backlogs and channel rates when applied to wireless networks [5] To this end, it presumes that all nodes obey the algorithm rules of information exchange, optimal link activation, and flow selection. However, in practice, a node may deliberately violate any rule to break the underlying premise assumed by the backpressure algorithm. For the secure data transmission embedding the secret information was used for sharing secret data, embedding process cryptography method plays a key role. And also trusted node was created for optimizing the data and transfers it in a secure way.

## 2. LITERATURE REVIEW

Yaghmaee MH, Adjerohb DA [6] Congestion control is an important issue in transport protocols. Congestion is also a difficult problem in wireless sensor networks. It not only wastes the scarce energy due to a large number of retransmissions and packet drops, but also hampers the event detection reliability. Congestion in WSNs and WMSNs has a direct impact on energy efficiency and application QoS. Two types of congestion could occur in sensor networks. The first type is node-level congestion that is caused by buffer overflow in the node and can result in packet loss, and increased queuing delay. Not only can packet loss degrade reliability and application QoS, but it can also waste the limited node energy and degrade link utilization. In each sensor node, when the packet-arrival rate exceeds the packet service rate, buffer overflow may occur. This is more likely to occur at sensor nodes close to the sink, as they usually carry more combined upstream traffic. The second type is link-level congestion that is related to the wireless channels which are shared by several nodes using protocols, such as CSMA/CD (carrier sense, multiple accesses with collision detection). In this case, collisions could occur when multiple active sensor nodes try to seize the channel at the same time.

Melodia et al [7] Earlier works in the field of sensing networks are mainly concerned with two qualitative differences, which include congestion reduction. So, the following problems are caused as a result of congestion reduction. In a sensing network, if the sensors are provided to sense environmental data, send them at certain periods, then if data traffic exceeds network capacity, nodes order and thus network output will determine justice degradation. It is different from congestion control, because finding the sensor nodes with higher justice has the highest impact on the process. In this case, the nodes transmit the information at an optimal rate, network is most efficient and the output of each node is close to the sent value. Adaptive Roll Control (ARC) indicates packet injecting to traffic flow like straight route traffic. Each node estimates the number of nodes in the neighborhood of Sink and the bandwidth is divided between straight route traffic and local traffic based on their priority. Division bandwidth of each node is an effort to achieve approximate justice. Reduction in the straight traffic transfer also affects upper nodes, which can reduce transmission rate.

S.Lavanya [8] Reliable delivery depends on probability of success and the ratio of packets sent to the packets received. Therefore for a successful delivery of data, various combinations of retransmission, redundancy techniques are to be followed. As suggested by author, cost and overhead need to be considered for every option that is followed. By increasing the no of parity bits, reliability is increased and the probability of packet loss is decreased. But there is a considerable increase in computation cost and overhead. Moreover erasure codes and other systematic codes needs to be modified according to the current trends of sensor networks. Retransmission and use of alternative route options are used only on-demand thereby reducing the cost.

Revathi Venkataraman [9], Wireless Sensor Networks (WSN) shows that the VAR trust model is suited for resource constraint networks. The backpressure scheduling is known for being throughput-optimal. However, it is usually assumed that nodes cooperate with each other to forward the network traffic. In the presence of malicious nodes, the throughput optimality no longer holds and this affects the network performance in collection tree applications of sensor networks. We apply an auto regression based scheme to embed trust into the link weights, making it more likely for trusted links to be scheduled. The novelty in our approach is that the notion of trust can be easily incorporated in a new state of the art distributed and dynamic routing Backpressure Collection Protocol in sensor networks. We have evaluated our work in a real sensor network testbed and shown that by carefully setting the trust parameters, substantial benefit in terms of throughput can be obtained with

minimal overheads. Our performance analysis of VAR in comparison with other existing trust models demonstrate that even when 50% of network nodes are malicious.

## 3. PROPOSED SYSTEM

The backpressure algorithm is known to provide throughput optimality in routing and scheduling decisions for multi-hop networks with dynamic traffic. The essential assumption in the backpressure algorithm is that all nodes are benign and obey the algorithm rules governing the information exchange and underlying optimization needs. Nonetheless, such an assumption does not always hold in realistic scenarios, especially in the presence of security attacks with intent to disrupt network operations. In this paper, we propose a novel mechanism, called distributed cluster-based back-pressure routing algorithm, to protect backpressure based routing and scheduling protocols against various insider threats. Our objective is not to design yet another trust-based routing to heuristically bargain security and performance, but to develop a generic solution with strong guarantees of attack resilience and throughput performance in the backpressure algorithm. To this end, we quantify a node's algorithm-compliance behavior over time and construct a virtual trust queue that maintains deviations of a give node from expected algorithm outcomes. We show that by jointly stabilizing the virtual trust queue and the real packet queue, the backpressure algorithm not only achieves resilience, but also sustains the throughput performance under an extensive set of security attacks. Our proposed solution clears a major barrier for practical deployment of backpressure algorithm for secure wireless applications.

a. Monitoring Neighbors

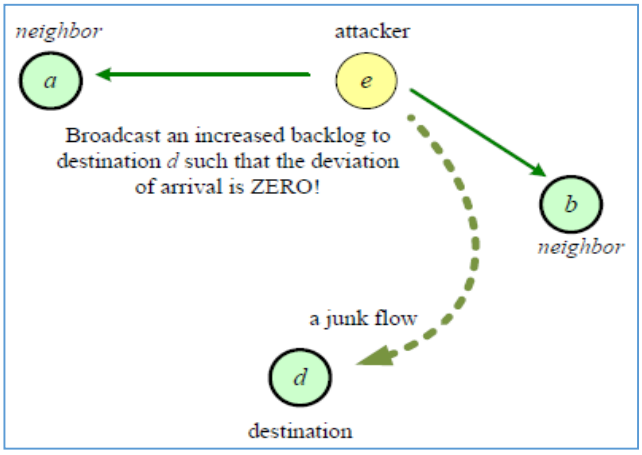


Figure 2: transmitting the path neighbor node when analyzing the attackers in that path

They detect these attacks by monitoring neighbors for behavioral anomalies and quantifying these results into direct trust metrics. Through this mechanism, the misbehaving neighbors are easily identified and alternate routing mechanisms are employed to achieve reliable communication in the network with minimum loss of resources. Although numerous cryptographic and statistical schemes are presented in the literature for wireless networks, there is no implemented work on practical systems related to trust models with dynamic backpressure routing in WSN.

This may be due to constraints like computational overheads, large delays and packet losses in these networks [11]. Addressing these concerns, we present the first implemented work on Vector Auto Regressive (VAR) trust model for WSN that works with dynamic backpressure routing.

b. Packet transmission

Confidentiality refers preventing the data packets from any unauthorized access. So here we discuss a scheme which makes the data transmission secure from base station to sender node [12]. Hash number is generate which spread through all over the network to make data transmission authenticate. Proposed an enhanced interleaved authentication scheme called the key inheritance-based filtering that prevents forwarding of false reports. Basically to make the data transmission secure first we have to maintain two basic fields these are – Authentication and confidentiality. Authentication means it has to make sure that data packet comes from the intended sender or packet received by the intended receiver those which are involved in the transmission process

c. Secure data transmission

After initializing the hash number and getting the hash number by all the nodes which is sent by the base station now all the nodes ready to start data transfer securely. If the packet is not validated after the verification process has been performed w times, intermediate nodes simply drops the packet. . In this paper, we propose a novel mechanism, called back-pressure routing algorithm, to protect backpressure based routing and scheduling protocols against various insider threats. Our objective is not to design yet another trust-based routing to security and performance, but to develop a generic solution with strong guarantees of attack resilience and throughput performance in the backpressure algorithm. To this end, we quantify a node's algorithm-compliance behavior over time and construct a virtual trust queue that maintains deviations of a give node from expected algorithm outcomes. We show that by jointly stabilizing the virtual trust queue and the real packet queue, the backpressure algorithm

d. Back-Pressure Algorithm

We begin with a mathematical overview of the back-pressure (BP) algorithm. The time is slotted, with t denoting t th time slot. We represent the network by a graph G = (N , L), where N corresponds to the set of nodes in the network and L being the collection of links. We denote μ(n1,n2)[t] to be the

transmission rate (measured in packets/time-slot) of link (n1, n2) ∈ L between n1, n2 ∈ N at time t, and ~μ[t] = {μ(n1,n2)[t], (n1, n2) ∈ L}. Finally Γ is the convex hull of the collection of all feasible transmission rates in the network. We observe that ~μ[t] and Γ could depend on the interference model used for the network. Let f[s,d] denote the flow from s to d. F denotes the set of all flows. Let x[s,d] be the rate at which s generates data for d, and let ~x = {x[s,d] , [s, d] ∈ F}. Let C denote the capacity region of the network under Γ. Each node in the network maintains a queue for every other node in the network [31]. Let q j i [t] denote the length of queue for node j maintained at node i; the queue for node i maintained at i is assumed to be zero for all time slots, i.e. q i i [t] = 0 ∀t. In each time slot t, each node n obtains queue information from its neighbor m ((n, m) ∈ L). Define

$P^{j}_{(n,m)}[t] = q^{j}_{n}[t] - q^{j}_{m}[t]$.

Let $j_{(n,m)}[t] = \arg\max_j P^{j}_{(n,m)}[t]$.

In each time slot t, the network compute and ~μ[t] such that

$$\vec{\mu}[t] = \arg\max_{\vec{\mu}\in\Gamma} \left\{ \sum_{(m,n)\in\mathcal{L}} \mu_{(m,n)} P_{(m,n)}^{j_{(m,n)}[t]}[t] \right\}$$

This packet may take a loopy walk through the network and never arrive at its destination because no pressure gradients build up. This does not contradict the above analysis, because the network has at most one packet at any time and hence is trivially stable. It is also possible to implement backpressure subject to some pre-specified paths that can be used. This can restrict the capacity region, but might improve in-order delivery and delay.

## 4. EXPERIMENTAL RESULT

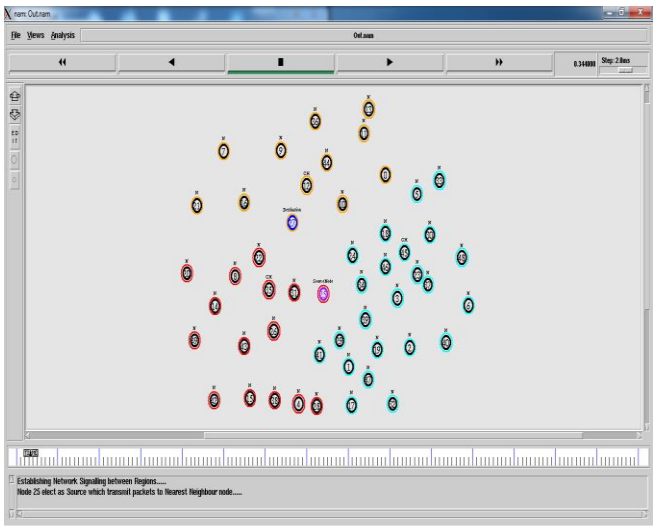

Fig 3: Node initialization

In this section, we conduct an extensive simulation study to evaluate the performance. Each node is half-duplex thus cannot transmit and receive at the same time. We adopt the protocol interference model; i.e., if two nodes are within each other's transmission range, their link rate is set to be 100 packets/s; otherwise, the rate is 0. In addition, if a node is receiving from a neighbor at a time slot, none of its other neighbors will be scheduled to transmit. There are in total 10 end-to-end flows with randomly selected source-destination pairs in the network.

This information might be conveyed over a wired or remote connection, or may go through a specific system customer.

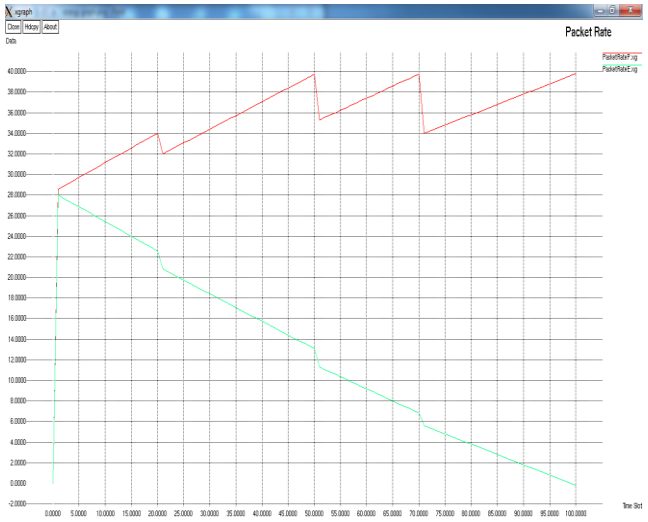


Fig 4: Packet rate transmission

Packet delivery ratio is calculated by ratio of packet received by the destination nodes to those generated by the source nodes. Hence the node density increases, the packet delivery ratio of dynamic path selection

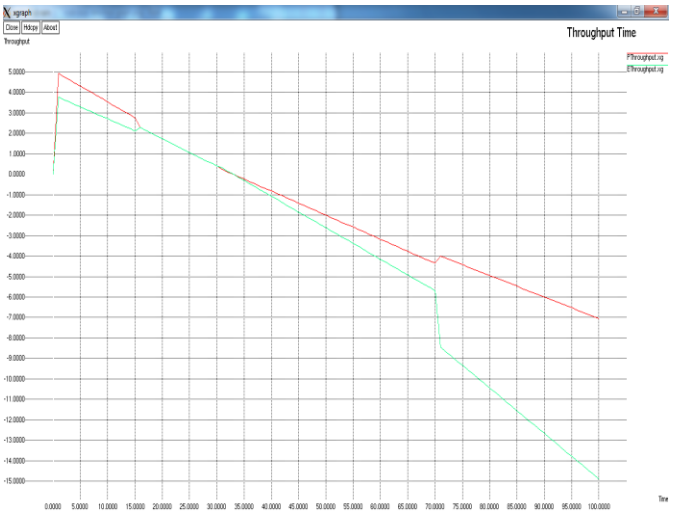


Fig 5: Throughput Rate

Sum is calculated by sending and receiving packet at the instance. In the notable time how many processes of segments of information it can be measured is calculated.

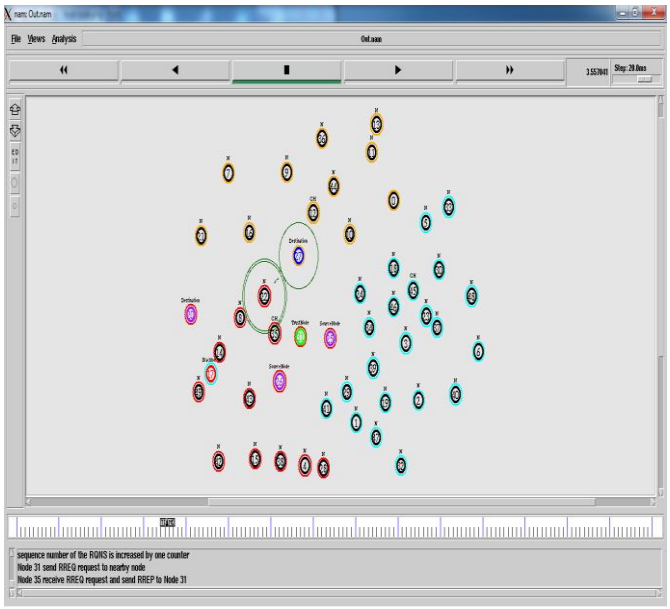

Fig 6: Attacker node

Initially when packet of data transmission is pretty high hence loss of which is gradually increasing. Then after this the packet of data losses increases accordingly.

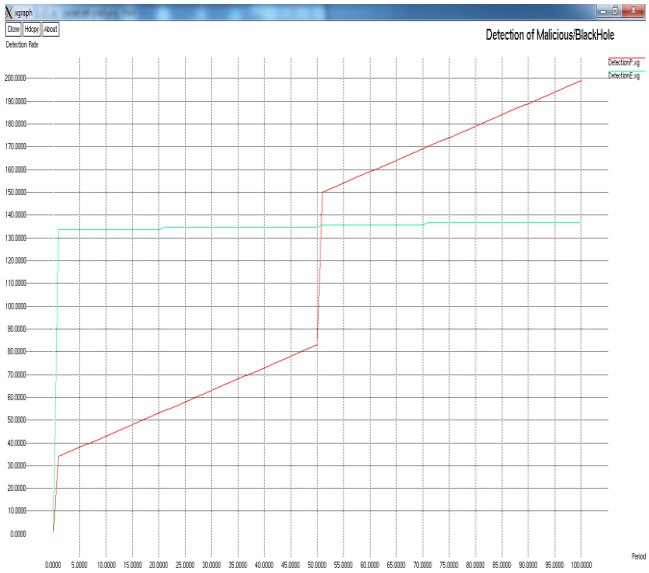


Fig 7: Malicious detection

## 5. CONCLUSION

In this paper we provide a data transmission by increasing throughput using backpressure algorithm. We also discussed how the data transmission can be secured and what are the main mechanisms is used to make the data transmission secure also how the broken path can be repair by re-initialization of trusted node. When compare to the existing one our proposed method plays a major role for the security issues, it provide the encrypted data and the secure data transfer. Existing method provide many drawbacks like one way transmission, increasing in waiting time response, data loss, etc. our proposed key attribute based method provide the better thing to solve those issues, it reduce the delivery time. Here we basically discussed how efficiently data transmission can be secured by some mechanisms. Here the optional key refreshment mechanism basically increase the level of security and ensure data freshness.

## REFERENCES

[1] Perrig, J. Stankovic, and D. Wagner, "Security in wireless sensor networks," *Commun. ACM*, vol. 47, no. 6, pp. 53–57, 2004.
[2] M. L. Das, "Two-factor user authentication in wireless sensor networks," *IEEE Trans. Wireless Commun.*, vol. 8, no. 3, pp. 1086–1090, Mar. 2009.
[3] Y. Zhou, Y. Zhang, and Y. Fang, "Access control in wireless sensor networks," *Ad Hoc Netw.*, vol. 5, no. 1, pp. 3–13, 2007.
[4] L. Ying, S. Shakkottai, A. Reddy, and S. Liu, "On combining shortest-path and back-pressure routing over multihop wireless networks," *IEEE/ACM Trans. Networking*, vol. 19, Jun 2011.
[5] S. Liu, L. Ying, and R. Srikant, "Throughput-optimal opportunistic scheduling in the presence of flow-level dynamics," *IEEE/ACM Trans. Networking*, vol. 19, Aug 2011.
[6] Yaghmaee MH, Adjerohb, Priority-based rate control for service differentiation and congestion control in wireless multimedia sensor networks. Computer Networks 2009; 53: 1798–1811
[7] Akyildiz I, Melodia WT, Chowdhury KR. "A survey on wireless multimedia sensor networks" Computer Networks 2007; 51:921–960
[8] S.Lavanya Reliable Techniques for Data Transfer in Wireless Sensor Networks
[9] Revathi Venkataraman, "Trust-based Backpressure Routing in Wireless Sensor Networks".
[10] Z. Lu, W. Wang, and C. Wang, "From jammer to gambler: Modeling and detection of jamming attacks against time-critical traffic," in *Proc. of IEEE INFOCOM*, 2011.
[11] R. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems". Communication of the ACM, pp. 120-126, 1978.
[12] Manika Sharma, Rekha Saraswat, "Secure Visual Cryptography Technique for Color Images Using RSA Algorithm", International Journal of Engineering and Innovative Technology (IJEIT) Volume 2, Issue 10, April 2013.
[13] Chunlin Jiang, Weijia JIA and Ke GU, "An Anonymous Wireless Authentication Protocol Based on Proxy Signature". Trans. 2012.