A Secure Congestion Adaptive Routing with Load Balancing for MANET

(IJCSNT) International Journal of Communication Systems and Network Technologies
ISSN Number: 2053-6283
Volume 1, Issue No. 3, 143–156

https://journals.mirlabs.in/index.php/ijcsnt
DOI- 10.18486/ijcsnt/1.3.012
IJCSNT

Laxmi Shrivastava[1], G. S. Tomar[2], Sarita S. Bhadoria[3]

Abstract

The main issue in ad hoc network is congestion, which occurs with limited resources and leads to packet losses, transmission delays and bandwidth degradation and also wastes time and energy on congestion recovery. Another issue in such networks is security - since every node participates in the operation of the network equally, malicious nodes are difficult to detect. To study these issues, a scenario based simulation analysis of a congestion adaptive and secure routing protocol is done and is compared with traditional non-congestion-adaptive and non-secure routing protocol i.e. Ad hoc On-demand Distance Vector (AODV) routing. In this paper, a load balanced congestion adaptive routing algorithm along with security (SLBCAR) has been proposed in which two metrics: traffic load density and life time associated with a routing path, have been used to determine the congestion status and weakest node of the route and the route with low traffic load density and maximum life time is selected for packet transmission. To analyze the performance of the system as per the proposed algorithm, AODV has been modified and simulated using Qualnet 4.5 and then compared with original AODV and DSR (Dynamic Source Routing).

Keywords

Ad Hoc Networks, Routing, Load Balance, Congestion Adaptive, Delay, Interference, Throughput, Wireless Networks, AODV, SLBCAR, DSR.

Received: 25 August 2012; **Revised:** 16 November 2012; **Accepted:** 25 November 2012; **Published:** 30 December 2012;

[1, 3]Department of Electronics, Madhav Institute of Technology & Science, Gwalior, Madhya Pradesh, India.
[2]Machine Intelligence Research Labs, 223 New Jiwaji Nagar, Gwalior, Madhya Pradesh, India.

Corresponding author:
Email: lselex@yahoo.com

Introduction

A Mobile Ad-hoc NETwork (MANET) is an autonomous collection of mobile users that communicate over relatively bandwidth-constrained wireless links. With the advance of the wireless communication technologies, small size and high performance computing and communication devices have been increasingly used in daily life and computing industry (e.g., commercial laptops and personal digital assistants equipped with radios). Wireless infrastructure-based networks place as much of the processing burden as possible on fixed sites with large power resources. For these networks all processing and control must be performed by the network nodes in a distributed fashion, making energy-efficiency challenging to achieve. Energy is a particularly critical resource in networks where nodes cannot recharge their batteries, for example in sensing applications.

A mobile ad hoc network (MANET) is a collection of mobile nodes that form a wireless network without the use of a fixed infrastructure i.e., base stations or access points or any centralized administration. Ad hoc wireless networks are self-creating, self-organizing, and self-administering, since the mobile nodes in the network dynamically establish routing among themselves to form their own network "on the fly" as in figure 1. Limited capabilities of mobile stations require a control on node congestion due to message forwarding and limited battery consumption. Efficient utilization of energy is one of the important concerns as nodes are battery operated. Energy efficiency continues to be a key performance metric as efficient utilization of energy increases the network longevity.

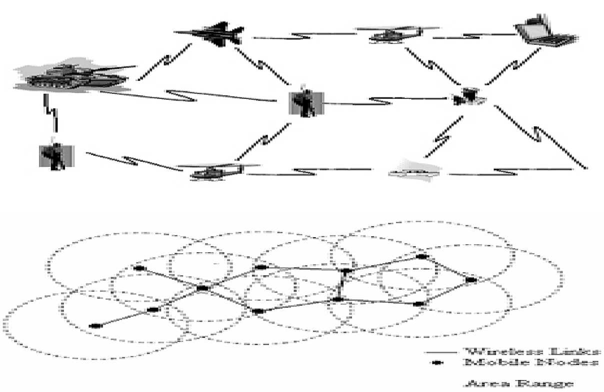

Figure 1. Overview and schematic diagram of Mobile Ad Hoc Network

Congestion in mobile adhoc networks is a situation in which too many packets are present in (a part of) the subnet, performance degrades. Congestion results from applications sending more packets then the network devices (i.e. router and switches) can accommodate, thus causing the buffers on such devices to fill up and possibility overflow. This can result in delayed or lost packets, thus by adding more traffic and further increasing the congestion. In order to reduce congestion, the routing protocol should reduce the number of packets in the network; however, simply dropping overflowed packets will reduce the data fidelity and increase the energy dissipation. Various techniques have been developed in attempt to minimize congestion in communication networks. In addition to increasing capacity and data compression, they include protocols for informing transmitting devices about the current levels of network congestion and reroute or delay their transmission according to congestion levels[7]. Congestion is a global issue, involving the behavior of all the hosts, all the routers, the store-and-forward processing with in the routers, etc.

Most of the on-demand protocols use the shortest path as their route selection metric. This scheme of route selection leads to congestion of some of the nodes in the network. The different multi-path schemes proposed earlier concentrates few of the performance aspects[5]. In addition to that, a mere use of multi-path routing schemes could adversely affect the network life as the depletion rate of battery power will be higher. Hence, setting a threshold value is critical to trigger multi-path routing as and when congestion occurs to balance the network life and improve the performance[13].

Most of the existing routing protocols do not consider the load conditions and residual battery energy at the nodes during the route setup phase; hence they are unable to take advantage of the less loaded and strongest nodes in the network topology. Routing with load balancing in wireless networks has been exploited in several schemes. In ad hoc networks, Associatively Based Routing (ABR) considers the load as the primary performance metric. The DLAR protocol[8], on the other hand uses the number of packets buffered in the interface as the primary route selection criteria. But the interface queue length alone does not give a true picture of the actual load in 802.11 MAC based protocols.

Security is a great issue in networks especially in MANETs where security attacks can affect the nodes limited resources and consume them, or yelled to loose the communication sessions, or waste the time before route chain broke. A wide variety of security attacks can be found in MANETs. Security is a vectored term of multi systems, procedures and functions that works together to reach certain level of security attributes namely Authentication, Integrity, Confidentiality, Availability, Access Control, and Non-repudiation[9]. Attacks from both external and internal nodes can easily affect the stability of the ad hoc networks. The degree of the influence depends largely on the active level of the malicious nodes. The time to recover the services relies on the detection of the mistakes or errors and responding policy.

In this paper, a new load balanced congestion adaptive technique along with security solutions has been proposed to reduce congestion and to maximize the network operational lifetime. The metric traffic load density is used to determine the congestion status of the route and link cost is used to determine the life time of the route. The route with low traffic load intensity and maximum life time is selected for packet transmission and this algorithm practically limits the idealized maximum number of packets transmittable through the route having weakest node with minimum life time and high traffic load intensity[10]. In this paper, group signature mechanism for security has been applied along with load balanced congestion adaptive algorithm.

This paper is organized as follows: in section II the protocols related to this proposed work have been discussed. In section III, detailed description of the proposed algorithm has been discussed. Section IV describes the simulation framework of the network. In Section V, simulation results have been investigated and analyzed. Section VI concludes this paper and defines topics for further research.

Related Work

Xiaoqin Chen, Haley M. Jones, A .D .S. Jayalath[1] proposed a congestion aware routing protocol for mobile ad hoc networks which uses a metric incorporating data-rate, MAC overhead, and buffer delay to combat congestion. Yung Yi and Sanjay Shakkottai[2] developed a fair hop-by-hop congestion control algorithm with the MAC constraint being imposed in the form of a access time constraint, using an optimization-based framework. Xuyang Wang and Dmitri Perkins[3] presented a cross-layer hop-by-hop congestion control scheme designed to improve TCP performance in multihop wireless networks. Duc A. Tran and Harish Raghavendra[4] proposed a congestion-adaptive routing. Sung-Ju Lee and Mario Gerla[8], proposed three Dynamic Load Aware Routing (DLAR) protocols that considers intermediate node routing loads as the primary route selection metric and also monitor the congestion status of active routes and reconstructs the path when nodes of the route have their interface queue overloaded. Yi Lu, Weichao Wang and Bharat Bhargava proposed a congestion-aware distance vector (CADV) routing algorithm[11] based upon the idea of integrating congestion avoidance mechanisms with proactive routing protocols to improve routing performance. Duc A. Tran and Harish Raghavendra[14] presented a routing with congestion awareness and adaptivity in MANETs (CRP) which tries to prevent congestion from occurring in the first place and be adaptive should a congestion occur. Basavaraju T G, C Puttamadappa, Subir kumar Sarkar[6] proposed an Efficient Congestion Adaptive Routing Protocol (ECARP) for MANETs designed to ensure the high availability of alternative routes and reduce the rate of stale routes and also reduce the rate of broken route removal process by increasing the parameters of the routing protocols (especially in AODV) such as active_route_time-out, route_reply_wait_time, reverse_route_life, TTL_start, TTL_increment, TTL_threshold and delete_period that normally take more time for link recovery.

B. RAMESH, D. MANJULA[19] presented a congestion adaptive adhoc on demand distance vector routing protocol. The main characteristics of the mechanism are its support of finding alternate route, in case of congestion on the primary route, on the basis of status of the buffer size of the neighbor and the status of the buffer size of the next node on the primary route. It diverts the incoming packets if the number of packets being queued at the interface queue of the node is more than 80% of its buffer size. A congestion aware routing protocol for mobile adhoc networks (CARM)[1] was proposed by Xiaoqin Chen, Haley M. Jones and A .D .S. Jayalath which employs the retransmission count weighted channel delay and buffer queuing delay, with preference of less congested high throughput links to improve channel utilization. Whenever streaming of multimedia based data such as video, audio and text is performed traffic will be more and network becomes congested in mobile adhoc networks. Boraiah RAMESH, Dhanabalachandran MANJULA[11] developed Congestion Adaptive AODV (CA-AODV) Routing Protocol for Streaming Video in Mobile Ad Hoc Networks that provides alternate non congested path if node becomes congested. The congested node will immediately provide congestion status to concerned node in order to take necessary action. S. Santhoshbaboo and B. Narasimhan[12] developed a hop-by-hop congestion aware routing protocol (CARP) which employs a combined weight value as a routing metric, based on the data rate, queuing delay, link quality and MAC overhead in its standard cost function to account for the congestion level. V. Saigal, A.K. Nayak and S.K. Pradhan proposed a new routing protocol called the LARA (Load Aware Routing in Ad hoc) networks protocol[13]. During the route discovery procedure, the destination node selects the route with the minimum traffic cost, which basically reflects the contention at the MAC level, for the non-TCP source. For TCP sources, it takes into account both the number of hops and the traffic cost of the route. This methodology of route selection helps the routing protocol to avoid congested routes. This helps to uniformly distribute the load among all the nodes in the network, leading to better overall performance. A. Valarmathi and R.M. Chandrasekaran proposed a congestion aware and adaptive DSR algorithm with load-balancing for MANET[14]. They presented a modified DSR protocol to monitor congestion or multiple resource utilization levels, notify the routing process of congestion and invoke multipath routing during the period of congestion. Z. Bin, Z. Xiao-ping, X. Xian-sheng and C. Qian proposes a novel adaptive load balancing routing algorithm in Ad hoc networks based on a gossiping mechanism (ALBR-G)[15]. This algorithm adjusts the forwarding probability of the routing messages adaptively, according to the load status and the distribution of the nodes in the phase of route discovery which reduces the routing overhead, and balances the load effectively.

It has been found from the research survey for congestion adaptive algorithms that there are still many issues in applying bypass routing techniques into mobile ad hoc networks that are still to be covered. In most of the routing protocols, the traffic is distributed mainly on the primary route. It is only when this route is broken that the traffic is diverted to alternate routes. Most of the existing routing protocols do not consider the load conditions at the nodes during the route setup phase; hence they are unable to take advantage of the less loaded nodes in the network topology. This results in poor performance of mobile ad hoc network. Although there are some routing protocols which distribute traffic simultaneously on multiple paths, there has not been any routing algorithm which could dynamically cope with the changes of traffic load and life time of the network.

Therefore in this paper, a congestion adaptive routing has been proposed that not only efficiently can balance the load on the network but also can cope with the dynamics of the network and increase the lifetime of the network. The adaptive concept of the network will certainly reduce the packet loss and thus increase throughput of the network.

Considering various security issues of AODV routing protocol several secure AODV routing protocol has been proposed featuring variety of advanced mechanism for securing data and control information. SAODV[16,17] (Secured Ad hoc On Demand Vector routing) is one of the popular existing secured mechanism which takes help of digital signature and hash chain techniques to secured AODV packets. SAODV enables each node to sign an outgoing message with its own secret key and verify all incoming message with the public key shared by other nodes. Since, digital signature technique is based on asymmetric key cryptographic method, heavy amount of computational time is required for signature and verification mechanism, and hence it affects the performance of SAODV protocol.

Since SAODV has been proved to be free of most of the security issues of AODV protocol, our objective is to propose some changes in routing behaviour of SAODV which in turn will improve its performance in term of performance metrics[18,19]. In a recent work called A-SAODV[12] (Adaptive SAODV), an adaptive mechanism that tunes the behaviour of SAODV to improve its performance. It makes an adaptive decision whether to reply an incoming request based on the load threshold value of the current node provided it has a valid and fresh route to the requested destination. This decision helps to balance the load of intermediate nodes which are over-burdened by signing and verification task of incoming messages. In our paper we have proposed an extension to Adaptive-SAODV of the secure AODV protocol extension, which includes further filtering strategies aimed at further improving its network performance. We have analyzed the how our proposed algorithm can help in further improvement of performance in adaptive SAODV and also compared its performance with existing mechanisms using simulation.

Unlike the existing protocols the new concept of securing packet before injecting to network through node has been proposed in this work. The traditional security protocols are providing limited security in the network and if nodes are accessed by any means then there is no security for contents. But in the proposed method even if data is accessed by unauthorized entities, still data will be secured as packet has been provided with the high degree of security using group signature scheme. The proposed group signature mechanism for security has been applied along with load balanced congestion adaptive algorithm and implemented in this work.

Proposed Work

SLBCAR (proposed protocol) requires that each node maintain a record of the latest traffic load estimations at each of its neighbors in a table called the neighborhood table. This table is used to keep the load information of local neighbors at each node. SLBCAR is a new load balanced congestion adaptive technique proposed to reduce congestion and to maximize the network operational lifetime. The metric traffic load density is used to determine the congestion status of the route and link cost is used to determine the life time of the route. The route with low traffic load intensity and maximum life time is selected for packet transmission and this algorithm practically limits the idealized maximum number of packets transmittable through the route having weakest node with minimum life time and high traffic load intensity.

It is assumed that there is no unidirectional links in the network. Node x_i samples the interface queue length in the MAC layer periodically. The interface queue length is the number of packets waiting buffered at that node for transmission over its wireless network interface. $q_i(j)$ is the jth sample value, and N is the sampling time over a period of time, then the traffic load of node x_i is defined as following[15]:

$$\mathit{Traffic\ Load}(i) = \left\{ \sum_{j=1}^{N} q_i(j) \right\} / N \tag{1}$$

Traffic Load (i) can be obtained from the information table of adjacent nodes.

The total length of interface queue of node x_i in the MAC layer is $q_{\max}(i)$, then the traffic load intensity function of node x_i is defined as following:

$$\mathit{Traffic\ Load\ Intensity}(i) = \mathit{Traffic\ Load}(i)/q_{\max}(i) \tag{2}$$

The link cost for a link (i, j) contains two parameters: a node specific parameter i.e. P_i and a link specific parameter i.e. $E_{i,j}$ and is defined as

$$L_{i,j} = P_i / E_{i,j} \tag{3}$$

Where P_i is the residual battery energy of the node and $E_{i,j}$ is the energy required to transmit a data packet of given size over link (i, j). $E_{i,j}$ is measured as

$$E_{i,j} = e_{i,j} / \left\{ (1-p)^k \right\} \tag{4}$$

Where $e_{i,j}$ is the energy involved in a single packet transmission, n number of hops in retransmission and $k = 1$ if hop-by-hop retransmissions are performed. In case of end-to-end retransmissions, for a path from a source node S (indexed as node 1) to node N that consists of $N-1$ intermediate nodes indexed as $2, 3, \ldots, N-1$. Hence $n = 2, 3, \ldots,$ and is chosen to be identical for all links. Clearly, if the exact path length is known and all nodes on the path have the identical link error rates and transmission costs, k should be chosen equal to that path length. p is the packet error probability given by

$$P = 1 - (1 - \mathrm{BER})^L \tag{5}$$

L is the packet size in bits. BER is bit error rate. Let the number of neighboring nodes of x_i is n, and all the traffic load intensity functions are known. These n values are sorted in the ascending order, and get a sequence number named as $\mathrm{seq}(m)_i$ $\{1 \leq \mathrm{seq}(m)_i \leq n\}$ corresponding to the Traffic Load Intensity (i) of x_i. Since $L_{a,b} \geq 1$, the forwarding probability of the data for the node x_i is given by the following expression:

$$p_i = 1 - \left\{ \frac{\mathrm{seq}(m)_i}{n\, L_{a,b}} \right\} \tag{6}$$

p_i is related to the existing traffic load of neighboring nodes. It depends on the relative size of the traffic load intensity of x_i in local region. The smaller the relative traffic load intensity is, the larger the forwarding probability will be, and the node will join the route preferentially; on the other hand, the node with relative heavier traffic load is of smaller forwarding probability of data, hence the probability of joining the route is reduced. In ad hoc networks, the density of nodes varies from areas. From this above equation, it is clear that where the density is higher (that means n is larger), p_i is smaller, thus the redundant forwarding of data and the routing overhead are reduced. Where the node density is lower, p_i is larger, thus the probability of route establishment is increased. From the analysis above p_i is able to adjust adaptively according to the nodes distribution in local region and the relative size of the traffic load. The redundant transmission of the routing messages is reduced and the network traffic load is balanced at the same time. p_i is also related to the link cost. Smaller the link cost (i.e. the route with weak node), smaller will be the probability to forward data. Higher the link cost (i.e. the route with strong node), the probability to forward packet to this route is high. Thus network life time is maximized.

In this way, traffic is splitted according to the traffic load intensity and link cost. The overloaded nodes are protected by using the nodes of lighter traffic load to establish the route, so as to balance the network load, lessen the congestion of the network, improve the data transmission efficiency and maximizes the network life time.

Therefore the route with low relative traffic load intensity and minimum link cost is selected to forward the packets. Thus the overloaded nodes are protected by using the nodes of lighter traffic load to establish the route, so as to balance the network load, lessen the congestion of the network, improve the data transmission efficiency and maximize the network life time.

Group Signature Security Scheme

Group signature scheme was introduced by Chaum and Van Heijst[21]. It allows any member of a group to digitally sign a document on behalf of the group in a manner such that a verifier can confirm that it came from the group, but does not know about the member who signed the document. A secure group signature scheme must satisfy the following properties[23]: correctness, anonymity, unlinkability, unforgeability, exculpability, traceability and coalition-resistance. A group signature scheme is comprised of the following procedures[22]: setup, join, sign, verify and open:

RSA is an algorithm for public-key cryptography that is based on the presumed difficulty of factoring large integers, the factoring problem. RSA stands for Ron Rivest, Adi Shamir and Leonard Adleman, who first publicly described it in 1978. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message.

Let p' and q' be distinct primes of equal bit length, such that both $p = 2p' + 1$ and $q = 2q' + 1$ are also prime. In this case, the number $n = pq$ is called a safe RSA modulus. The multiplicative group of quadratic residues modulo n is denoted by $QR_{(n)}$, which is a cyclic group of order $p'q'$. The flexible RSA problem is defined as finding a $u \in QR_{(n)}$ and an integer e, $e > 1$, such that $u^e = y \bmod n$, for given y and n. Solving the flexible RSA problem is easy if one knows the prime factorisation of n. The strong RSA assumption states that given only y and n, the flexible RSA problem is hard to solve.

This concept has been used with the message put as payload in the secure packet having frame format with secure signatures. The length of message packet increased due to overheads of proposed secure algorithm. The timestamp is used to ensure that the message is freshly generated instead of a duplicate of a previous one. The frame format is as follows:

Table 1. Format of safety packet: fields and lengths

Group ID	Payload	Timestamp	Signature
2 bytes	512 bytes	4 bytes	368 bytes

Simulation Framework

Simulation Setup

The simulations of network have been carried out using Qualnet 4.5[20]. Each mobile node uses a Two-Ray ground radio propagation model with omnidirectional antenna. The simulations assumed an IEEE 802.11b network configured with 100 nodes uniformly distributed over a 1500m×1500m area, moving according to a random way point model with a maximum speed of 20 m/s and packet rate is 4 packets per second. The simulations were run for 300 seconds with 25 and 50 CBR connections (means 25 and 50 transmission links) and for each connections, the source generated 886 bytes data packets. The initial battery capacity of each node assumed to be 100%. The battery capacity of a mobile node was decremented in a predefined manner by the txPower and rxPower levels which remains constant throughout the simulation. The node pauses for a period before repeating the same process. That duration is known as pause time. The performance of the network was evaluated by varying pause time with values 20, 40, 60, 80, 100 and 120 sec and number of packets sent by sources to be 100.

Performance Metrics

In this paper, the performance metrics such as throughput, packet delivery ratio, average end-to-end delay and average jitter were calculated and evaluated for original AODV, DSR and modified AODV.

Throughput

Throughput is the measure of the number of packets successfully transmitted to their final destination per unit time.

Packet Delivery Ratio

Packet Delivery ratio is the ratio of the number of data packets successfully received at the destinations to the number of data packets generated by the sources.

Average end-to-end delay

The average end-to-end delay is a measure of average time taken to transmit each packet of data from the source to the destination. Higher end-to-end delay is an indication of network congestion.

Average Jitter

Jitter is the variation in the time between packets arriving, caused by network congestion, timing drift or route changes.

Simulation Results

The routing proposed in this paper is congestion adaptive so that congestion can be reduced in advance. The increase of CBR connections (transmission links) in the network will result in the increase in congestion. To investigate the effectiveness of the proposed routing and the effect of pause time on congestion, simulations have been carried out for 25 and 50 CBR connections at different values of pause time and results have been analyzed.

Results with 25 CBR connections

In this paper, the results have been presented by taking average over 10 runs of each simulation setting. Figures (3-6) show throughput, packet delivery ratio, average end-to-end delay and average jitter with varying pause time with 25 CBR connections. These figures show that proposed routing outperformed AODV and DSR, especially when traffic was heavily loaded in all respects. Data packet delivery ratio of proposed routing is greater than that of AODV and DSR. Packet loss due to congestion in DSR is more than AODV and SLBCAR at low pause time. Proposed routing delivered packets more successfully. In SLBCAR, congestion is better resolved and therefore, it offers less average end-to-end delay. It is very high for DSR as compared to AODV and SLBCAR. It resulted in less congestion because of no need to include entire information in data. Proposed routing introduces better improvement in

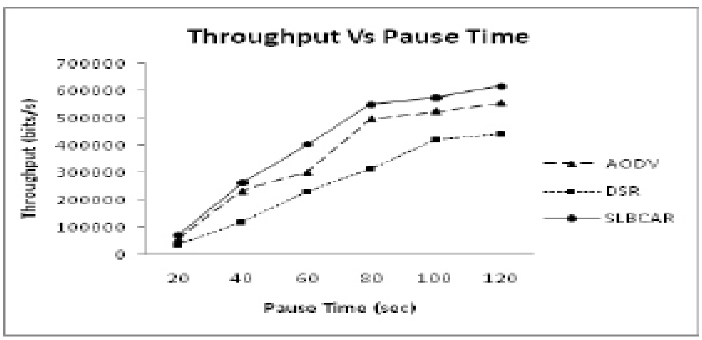

Figure 2. Throughput at different pause time with 25 CBR connections

throughput and packet delivery ratio at high pause time and average jitter and average delay at low pause time.

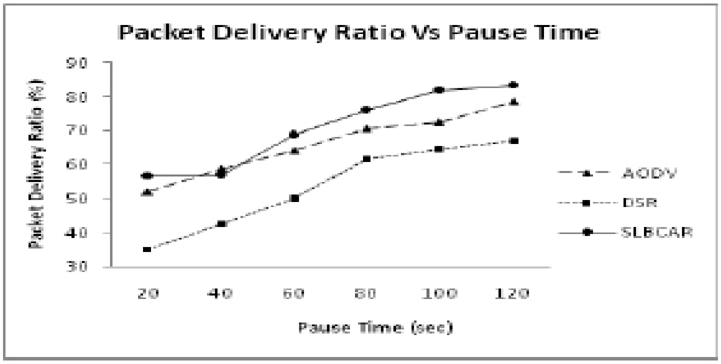

Figure 3. Data packet delivery ratio at different pause time with 25 CBR connections

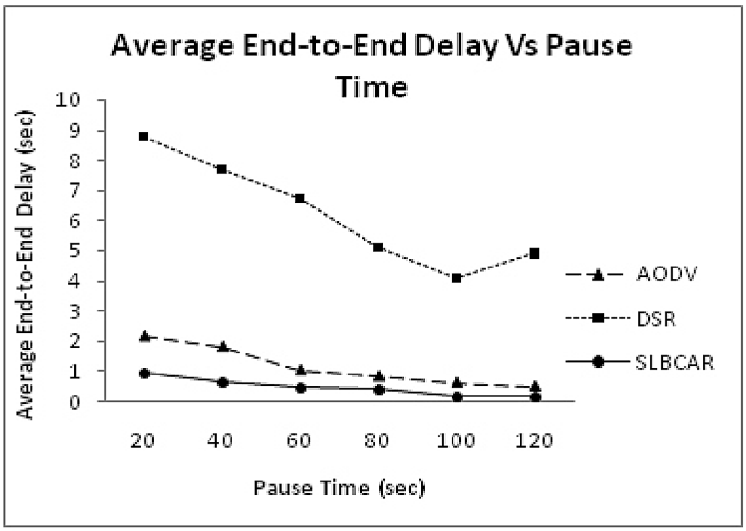

Figure 4. Average end-to-end delay at different pause time with 25 CBR connections

Results with 50 CBR connections

Figures (7-10) show throughput, packet delivery ratio, average end-to-end delay and average jitter with varying pause time with 50 CBR connections. SLBCAR is slightly better than AODV in all respects but as the number of connections is more, so the improvement in the performance of SLBCAR is slightly low as compared to the improvement for 25 CBR connections. The difference between SLBCAR and AODV in terms of delay and jitter vey small. The increase in jitter values with low pause time is primarily due to the increase in traffic flow among the multi-path.

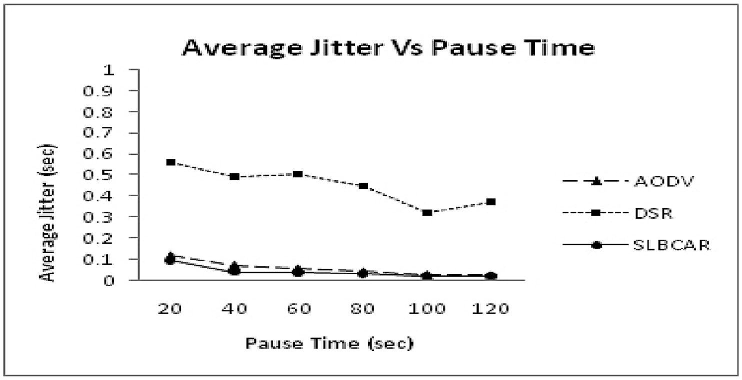

Figure 5. Average jitter at different pause time with 25 CBR connections

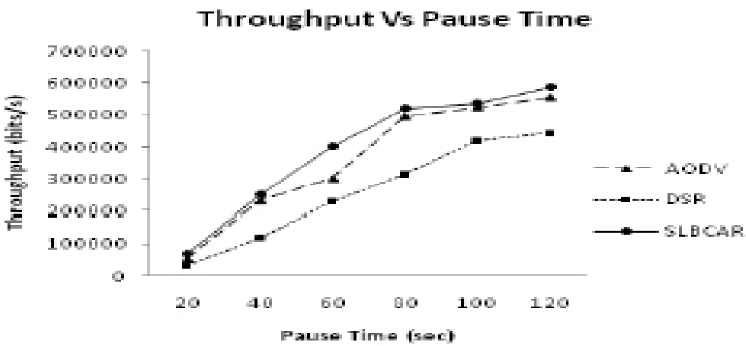

Figure 6. Throughput at different pause time with 50 CBR connections

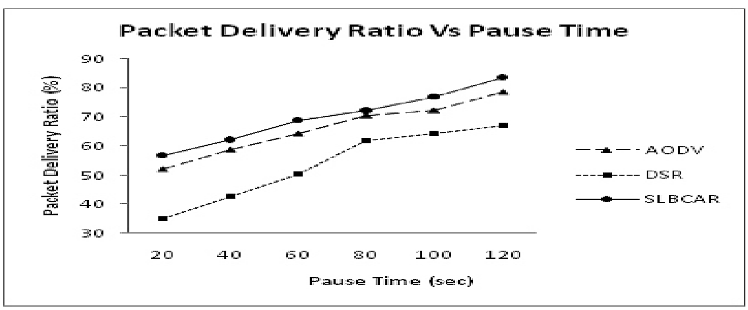

Figure 7. Data packet delivery ratio at different pause time with 50 CBR connections

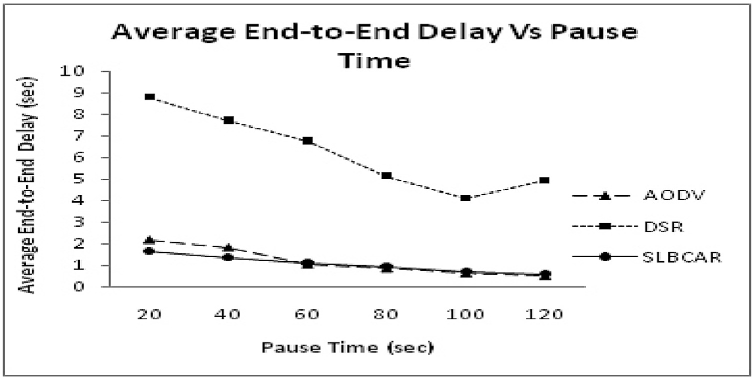

Figure 8. Average end-to-end delay at different pause time with 50 CBR connections

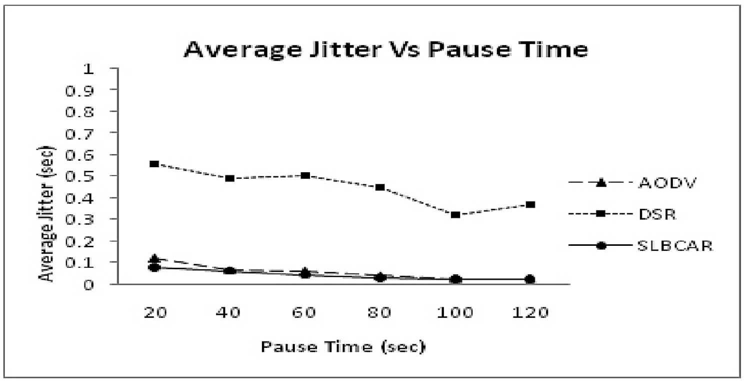

Figure 9. Average jitter at different pause time with 50 CBR connections

Conclusion

This algorithm combines the idea of load balanced congestion adaptiveness and security effectively. It can adaptively adjust the forwarding probability of RREQ messages according to the distribution and load status of nodes in route discovery phase. Simulation results indicate that, compared with original AODV and DSR, SLBCAR (modified AODV) can significantly reduce the end-to-end delay and jitter and enhance the throughput and packet delivery ratio and balance the load in the network. The performance of AODV is better than DSR and SLBCAR outperforms AODV.

The AODV protocol does not consider the load condition of the nodes during route setup. This leads to high contention at the MAC layer in some of the centrally located nodes, resulting in high end-to-end delay and increased probability of congestion. The SLBCAR protocol on the other hand makes a better route selection than DSR, and shows a remarkable improvement in performance. SLBCAR protocol makes an enhanced route selection attempt based on traffic load intensity and link cost which leads to better performance than AODV and DSR as far as throughput, end-to-end delay, jitter and packet delivery fraction are concerned. This is so because SLBCAR balances the load among all the nodes in the network topology and thus prevents excessive queue build up and consequent packet drops, i.e. congestion.

References

[1] Xiaoqin Chen, Haley M. Jones and A .D .S. Jayalath, “Congestion-Aware Routing Protocol for Mobile AdHoc Networks”, in proceedings IEEE 66th Vehicular Technology Conference, 2007, pages pp. 21–25, Baltimore, MD, USA.

[2] Y. Yi and S. Shakkottai, “Hop-by-hop congestion control over a wireless multi-hop network”, Proc. IEEE Infocom, March 2004.

[3] Xuyang Wang and Dmitri Perkins, “Cross-layer Hop-by-hop Congestion Control in Mobile Ad Hoc Networks”, IEEE, 2008.

[4] Duc A. Trans and Harish Raghavendra, “Congestion Adaptive Routing in Mobile Ad Hoc Networks”, IEEE Transactions on Parallel and Distributed systems, Vol. 17, No. 11, pp 1294–1305, Nov. 2006.

[5] Y. J. Lee and G. F. Riley, “A workload-based adaptive load balancing technique for mobile ad hoc networks,” Proc. of WCNC, vol. 4, pp. 2002–2007, Mar. 2005.

[6] T G Basavaraju, Subir Kumar Sarkar, C Puttamadappa and M A Gautham “ECARP: An Efficient Congestion Adaptive Routing Protocol for Mobile Ad hoc Networks”, 6th International Conference on ITS Telecommunication Proceedings, 2006.

[7] M. Gerla, S.-J. Lee, “Dynamic load-aware routing in ad hoc networks”, Proceedings of IEEE ICC 2001, Helsinki, Finland, June 2001, pp. 3206–3210.

[8] C.E. Perkins and E.M. Royer, “Ad-Hoc On Demand Distance Vector Routing”, Proceedings of IEEE WMCSA’99, New Orleans, LA, February 1999, pp. 90–100.

[9] D.B. Johnson and D.A. Maltz, “Dynamic Source Routing in Ad Hoc Wireless Networks”, In Mobile Computing, edited by Tomasz Imielinski and Hank Korth, Chapter 5, Kluwer Academic Publishers, 1996, pp. 153–181.

[10] Yi Lu, Weichao Wang, Yuhui Zhong and Bharat Bhargava, “Study of Distance Vector Routing Protocols for Mobile Ad Hoc Networks”, proceedings of IEEE PerCom, 2003.

[11] B. RAMESH, D. MANJULA, “CA-AODV: Congestion Adaptive AODV Routing Protocol for Streaming Video in Mobile Ad Hoc Networks”, I. J. Communications, Network and System Sciences, 2008, 4, 285–385.

[12] S. Santhosh baboo and B. Narasimhan, “A Hop-by-Hop Congestion-Aware Routing Protocol for Heterogeneous Mobile Ad-hoc Networks” International Journal of Computer Science and Information Security (IJCSIS), Vol. 3, No. 1, 2009.

[13] V. Saigal, A.K. Nayak and S.K. Pradhan, “Load balanced routing in mobile ad hoc networks”, Elsevier, Computer Communication 27 (2004), 295–305.

[14] A. Valarmathi and RM. Chandrasekaran, “Congestion Aware and Adaptive Dynamic Source Routing Algorithm with Load-balancing in MANETs”, International Journal of Computer Applications (0975 8887), Volume 8 No. 5, October 2010.

[15] Z. Bin, Z. Xiao-ping, X. Xian-sheng and C. Qian, “A Novel Adaptive Load Balancing Routing Algorithm in Ad hoc Networks” Journal of Convergence Information Technology Volume 5, Number 5, July 2010.

[16] M. G. Zapata and N. Asokan, “Securing Adhoc Routing Protocols”, Proceeding 1st ACM Workshop, Wireless Sec., 2002, pp. 1–10.

[17] M. G. Zapata, “Secure Ad hoc On-Demand Distance Vector (SAODV) Routing, IETF Internet draft, September 2006, pp. 1–22.

[18] Davide Cerri, Alessandro Ghioni, “Securing AODV: The A-SAODV Secure Routing Prototype”, IEEE Communication Magazine, Volume 46, Issue 2, February 2008, pp. 120–125.

[19] Yuxia Lin, A. Hamed Mohsenian Rad, Vincent W.S. Wong, Joo-Han Song, “Experimental Comparisons between SAODV and AODV Routing Protocols”, Proceedings of the 1st ACM workshop on Wireless multimedia networking and performance modeling, 2005, pp. 113–122.

[20] Qualnet Simulator 4.5, www.scalable-networks.com.

[21] D. Chaum and E. van Heijst, “Group signatures,” in Proc. Advances in Cryptology - Eurocrypt’91, ser. LNCS, vol. 576. Springer-Verlag, pp. 257–265, 1998.

[22] Gouri Sankar Mishra, “A Novel Group Signature Scheme Without One Way Hash”, Thesis, National Institute Of Technology Rourkela, Orissa, India, 2010.

[23] Constantin Popescu, “An Efficient Id-Based Group Signature Scheme”.