IRACST – International Journal of Computer Networks and Wireless Communications (IJCNWC), ISSN: 2250-3501
Vol.2, No5, October 2012

SECURED QoS ROUTING PATH DISCOVERY IN WIRELESS ADHOC NETWORKS USING CACHE MECHANISM

Dr. THANGARAJ. P [1], RENUKA. M [2], Dr.SIVANANDAM S.N[3]

[1] Professor & HOD, Department of Computer Science and Engineering, Bannari Amman Institute of Technology, Sathyamangalam, Tamilnadu, India.E-Mail : ctptr@yahoo.co.in.

[2] Assistant Professor, Department of Applied Science, SSM College of Engineering, Komarapalayam, Tamilnadu, India. E-Mail :mr.renuka@gmail.com.

[3] Professor & HOD, Department of Computer Science and Engineering(Retired).

***Abstract* - Wireless ad-hoc networks consist of a set of nodes which construct a random network topology by means of several communication media. Wireless ad-hoc network present a diversification in communication technology necessary to solve the end-to-end requirements of the QoS based communication networks. Of the numerous confronts in the composite dispersed system, the difficulty of secure routing based on a predefined position of inclinations, decisive to promising quality-of-service, is the focus of this research. Our previous work describes the process of providing the Energy Conserved Fault Tolerant Clusters QoS Routing service to the wireless ad-hoc networks (ECFCR) in the way of clustering the network based on energy consumption, fault tolerance rate, and mobility rate. A wireless ad-hoc network is efficiently clustered and cluster head is chosen based on the nodes which have higher energy, less mobility rate and high fault tolerance rate. Even though ECFCR provides an efficient clustering process, security in QoS routing does not achieve. To enhance the secure routing in wireless ad-hoc network, in this work, we are going to present a new approach which provides an authorized routing path from source to destination. Routing security is done using cache mechanism to evade misdirecting malicious node. Link failures are guarded against adversary or selfish nodes. For each node in the network, cache history is maintained which provides authenticated routing link for specific source destination pairs. Authorized nodes in the ad hoc network delineate the inappropriate routing directions. This cache mechnaims will improve the QoS routing path based on mobile node preferences and minimizes the communication overhead. An experimental evaluation is carried out to estimate the performance of the proposed Secured QoS Routing Path Discovery using Cache mechanism [SRPDC] in wireless ad-hoc networks in terms of routing overhead, routing efficiency, and energy consumption.**

Key Words - Wireless Ad-hoc Networks, QoS routing, Security, Cache Mechanism

1. INTRODUCTION

An authentic type of wireless networks that has been emitted out is supported on an Ad Hoc topology in which these types of networks are called Wireless Ad Hoc Networks. The phrase wireless network signifies a computer network in which the transmission links are wireless. The phrase Ad Hoc derives from the process that there is no fixed infrastructure for sending the packets from source to destination. Figure 1 shows an instance of wireless ad-hoc network. The circle presents transmission ranges of separate nodes. In the real world, this circle boundary is never to be predicted as a perfect circle and the transmission links might even be unidirectional in several cases.

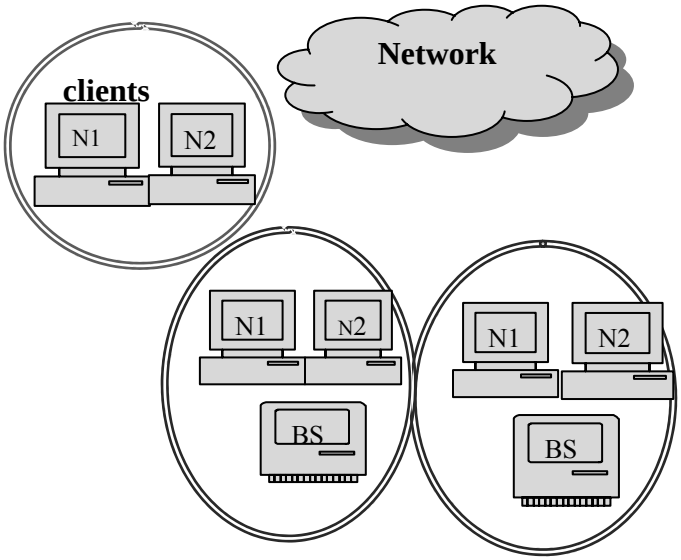

Figure 1. Ad-Hoc Network

In Ad Hoc networks, every node will send the data to other nodes, and so the process of checking of which nodes send data is made randomly supported on the network connectivity. This process is accessed in contrast to the infrastructure-based networks in which destination nodes, normally termed as routers, hubs, switches, and firewalls, process the assignment of sending the data. Ad-hoc network is utilized in situations like military conflicts, natural or human-induced disasters, emergency medical situations etc. since it requires minimal configuration and quick deployment.

QoS routing is significant in wireless ad-hoc networks. That is, in wired networks, overprovisioning is frequently employed to diminish the requirement for QoS techniques in all but the most promising network applications. Nevertheless, in wireless networks, overprovisioning is normally impractical, owing to restrctions on radio spectrum and power level, or since the network interference became less. Consequently, with QoS routing protocol, select the routing paths in the network with enormous amount of resources might be the only process to obtain requisite number of resources in wireless networks for several applications. This is even more significant in ad hoc networks owing to the subsequent number of modifications in routing topology and the requirement to expand the utilization of the shared resources over several wireless hops. With respect to the resources, current work on route identification reveals that link quality measurement precisely progress network performance even for best-effort packet traffic in the network environment.

Today security acts as a significant role in wireless ad-hoc network supported on the process of defense-in depth, where several layers are employed to secure ad-hoc network from malicious nodes. The network with high vulnerability needs a relaible secure communication; intrusion prevention mechanisms alone could not able to access the security requirements. Hence, Intrusion Detection Systems (IDSs), acts as an indispensable for ad-hoc networks with high security needs.

In this work, we are going to present a new approach which provides an authorized routing path from source to destination. Routing security is done using cache mechanism to evade misdirecting malicious node. Link failures are guarded against adversary or selfish nodes. For each node in the network, cache history is maintained which provides authenticated routing link for specific source destination pairs. Authorized nodes in the ad hoc network delineate the inappropriate routing directions.

2. LITERATURE REVIEW

In wireless ad-hoc networks, node mobility frequently fallout in common topology amends, which provides a considerable, confronts when scheming QoS routing procedures. It is inaccessible for elevated node mobility to convince QoS necessities. Therefore, it is essential that the network be combinatorial secure so as to realize QoS maintenance. Owing to the high plasticity, mobility and small cost features, wireless ad hoc networks are extensively employed. A chiefly demanding trouble is how to possibly notice and guard the main attacks beside routing protocols of such networks that contain vulnerable links and active topology. Most of the accessible safe routing procedures for ad hoc networks either evade the most demanding domestic assaults such as Byzantine behaviors, or have frequently formed ineffective security mechanisms. In [1], we suggest the method for protecting the QoS direction and to enlarge the possibility of achievement in deciding QoS possible paths.

In current years, the security concerns on MANET have turn into one of the principal apprehensions. MANETs rely on the collaboration of the nodes contributing in the network to promote packets for every other node in the network. Therefore, in [2], proposed a novel IDS architecture with agents and clusters which identify intermediary nodes disobedient and irregularities in packet on warding. Achieving Quality of Service (QoS) maintenance in Mobile Ad Hoc Networks (MANETs) [3] is a mainly dynamic study area with a amount of proposals to sustain real-time applications based ahead the communication among the routing system and a QoS provisioning system [4]. Consequently, routing procedures in wireless networks are more susceptible than routing procedures in wired networks. As of exclusive features of wireless networks, existing security approaches, particularly Intrusion Detection Systems (IDSs) like verification and encryption that planned for wired networks are not appropriate for wireless networks. The paper [5] constructs QoS-aware Shortest Multipath Source (Q-SMS) routing scheme.

Normally, the source node sustains the revealed path in its route cache and provides the packets to the destination node during the exposed route. If several links on a source path is wrecked, the source node is advised to employ a Route Error (RERR) packet [6]. Misbehaving nodes are nodes that have abnormalities in data swap prototypes. Define a pail as a precise calculation of packets that are broadcasted among two nodes [7] beside diverse types of attacks [8]. In [9], a novel QoS-aware routing system is planned which is supported on Shortest Multi-path Source (SMS) routing method. A dedicated ‘operation Monitor’ module is presented and incorporated into the IEEE implementation [10] inside network simulator. Cross layer cooperation is presented in wireless ad-hoc network to perform the accurate admissions of the nodes in the network [11] and the evaluation of the routing scheme is also being presented in paper [12]. In this work, we are going to

present a routing path discovery scheme to process an efficient route discovery in wireless ad-hoc networks.

3. PROPOSED SECURED Qos ROUTING PATH DISCOVERY IN WIRELESS ADHOC NETWORKS USING CACHE MECHANISM

The proposed work is efficiently designed to identify the secure routing path over wireless ad-hoc networks by adapting cache mechanism. Normally, Routing security is done to evade misdirecting malicious node. Link failures are guarded against adversary or selfish nodes. Node cache history maintains authenticated routing link for specific source destination pairs. Authorized nodes of ad hoc network delineate the inappropriate routing directions. The proposed Secured QoS Routing Path Discovery using Cache mechanism [SRPDC] in wireless ad-hoc networks is operated under two different phases. The first phase is to identify the secure path at first a node transfers packets from source to destination. The second phase describes the process of maintaining and implementing the cache mechanism to store the authorized route links and provide a link only to the authorized nodes in the network environment. The proposed secured QoS routing path discovery using cache mechanism is shown in Figure 3.1.

From the Figure 3.1, it is being observed that the routing security is done effectively with the cache mechanism. Routing security is done to evade misdirecting malicious node. Link failures are guarded against adversary or selfish nodes. Node cache history maintains authenticated routing link for specific source destination pairs. Authorized nodes of ad hoc network delineate the inappropriate routing directions which improve QoS routing path based on mobile node preferences, minimized communication overhead and reduces the node energy consumption on routing.

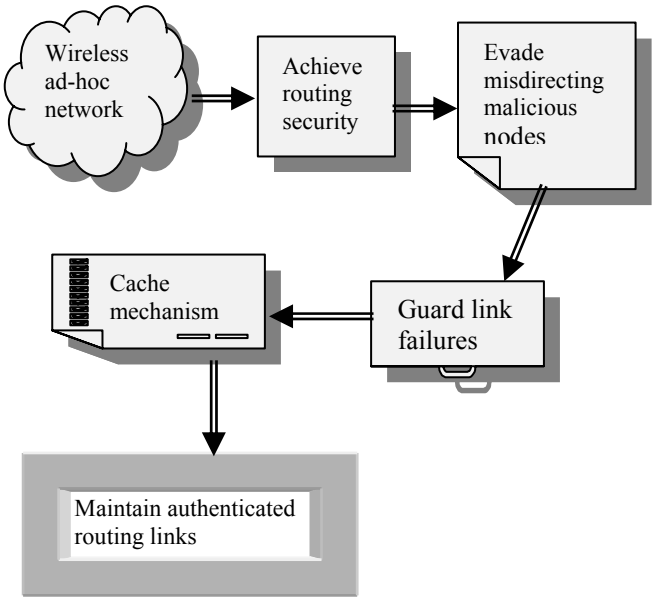

Figure 3.1 Architecture diagram of the proposed SRPDC

3.1 Specification of secure route discovery for QoS routing

Let N be the set of network nodes in wireless ad-hoc networks, and L the set of couples of discrete nodes specified as links. A route is a series of nodes $V_i \in N$, and links $l_{i,i+1}=(V_i, V_{i+1}) \in L$, for $0 \le i \le n-1$, i.e., route=$\{V_0, l_{0,1}, V_1, l_{1,2}, V_2,\ldots, V_{n-1}, l_{n-1,n}, V_n\}$. Specifying it as a route for series of nodes V_i requires that for some two successive nodes of the route $(V_i, V_{i+1}) \in L$. A route with $V_0 \equiv S$ and $V_n \equiv T$ an (S,T)-route. Let $f: L \rightarrow M \in R$ be a utility of assigning labels, to be precise, genuine values $f(l_{i,i+1})=a_{i,i+1} \in A$, to course edges $l_{i,i+1}$. Each label $a_{i,i+1}$, which we signify as a link metric, presents a quantitative explanation of the $l_{i,i+1}$ attribute(s).

The routing procedure input is a pair of nodes, P and Q, and the output is an (P,Q)-route; this is specified as basic routing protocol. An augmented routing protocol, with P and Q as input, and output an (P, Q)-route and a series of connection metrics, with one metric for every (P, Q) route connection. Then, the attributes of the complete path can be 'reviewed' by the collective charge of the connection metrics. The collective charge is considered by a utility g: $A \rightarrow R$ we denote as the route metric $g(a_0,a_1.,,,a_{n-1})$ The structure of g is reliant on the procedure, and believe four diverse forms. Furthermore, define i,i+1 to be the genuine metric value for connection $l_{i,i+1}$, and the aggregate $g(l_0,l_1.,,,l_{n-1})$ of the genuine connection metrics as the genuine path metric.

Let t_1 and $t_2>t_1$ be two points in instance that describe a time period (t_1, t_2), with time t_2 the period at which the routing procedure determines a route. We are concerned in routing procedures which guarantee three properties for the revealed route(s): freshness, loop-freedom, and accuracy. An (P,Q)-route is loop-free if it has no recurrences of nodes, and it is new with regard to the (t_1, t_2) period if every route's essential links is high at some point in point through the interval (t_1, t_2).

3.2 Broadcast authentication for route request packets

The mechanisms for safe and secure QoS Route detection need the network to present various structure of *transmit substantiation* for the unchallengeable fields of ROUTE REQUEST data packets; specifically, every node that obtains a ROUTE REQUEST data packet ought to be capable to establish that it was sent by the declared originator. Although this substantiation can be presented by a digital signature, the charge of confirming a digital signature generates the prospect of a Denial-of-Service (DoS) attack; an attacker overflows a sufferer node with unacceptable ROUTE REQUEST packets, forcing the

sufferer to devour all of its CPU point endeavoring to confirm the signatures on the REQUESTs. A substitute to the utilization of digital signatures is to present this substantiation using a proficient, direct transmit substantiation method such as HORS.

In SQoS, nevertheless, this substantiation is incorporated with a system that avoids disproportionate flooding. In meticulous, as QoSGuided path detection needs a overflow of the network and hence provides a means for an attacker to achieve a Denial-of-Service attack, a safe and secure ad hoc network routing procedure should implement restrictions on the occurrence at which every node can commence such flooding. The technique presented here has two merits. First, it permits every node to substantiate that a ROUTE REQUEST initiate from the originator. Second, it employs only proficient symmetric cryptography. Nevertheless, this method does not avoid alteration of the fields of the REQUEST. A node employs path detection, and utilizes the signature from that MW-chain step to substantiate the absolute fields of the ROUTE REQUEST.

3.3 Cache Mechanism

After identifying the authenticate route path by the sender among the nodes in the network environment. Once the route path is identified and acknowledges the route request packet by the receiver, then the node stores the path as an authenticated route path. If the node wants to send a packet to some other node, it will first checks with the cache and identifies the route path whether it is a correct route path or not. If it is a correct path, choose the path and send a packet from source to destination. The process of cache mechanism is shown in Figure 3.2.

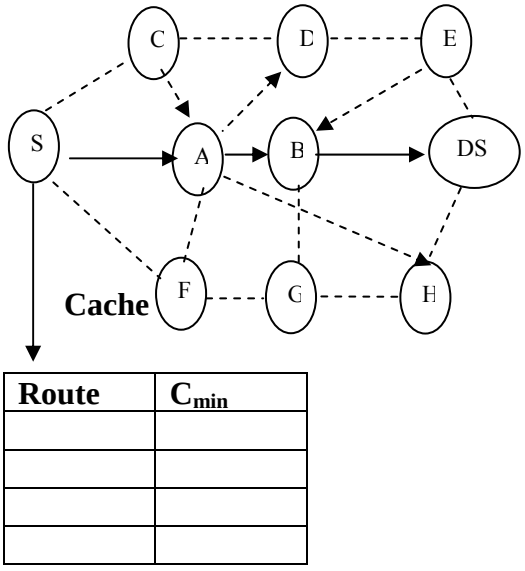

Figure 3.2 Process of cache mechanism in QoS route discovery

SPRDC is a secure QoS-aware routing system that employs a cache mechanism. Consequently, the routing method supported on the data packet submission necessities. SPRDC identifies a route from source to the destination by cache maintained by every node in the network with a QoS Route Request (QRREQ). SPRDC enlarges RREQ packet plan of data packet with the capacity restriction. The capability restraint comprises of the essential capability (C_{req}) and least obtainable capacity (C_{min}) presenting the greatest capability of the request and the least accessible capability of a leaving link practical for path collection. So QRREQ has the design:

$$QRREQ = RREQ \cup \{C_{req}, C_{\min}\} \qquad (1)$$

The source node reports C_{req} and compares the results with the restricted outstanding capability (C_{res}) of the leaving connection. If the value of C_{res} is upper than C_{req}, the source node reports the charge of C_{res} in the C_{min} field which, primarily is perpetuity and transmit the QRREQ packet to its neighbor nodes to identify an authenticated link. If the route path is identified and sent the packet efficiently to the destination, the link is stored and maintained at the respective node cache.

On receiving QRREQ packet, an intermediary node determines its enduring capability C_{res}. If the value C_{res} is higher than C_{req}, the node sends this QRREQ to the node. Or else this requested packet is discarded. Then the node also informs the C_{min} field if the value of C_{res} is lower than preceding C_{min}. The updates in route detection method to integrate permission control based on capacity estimation of the nodes in the network.

3.3.1 QoS Route Reply Phase

SPRDC extends RREP packet design of the source node RREQ pattern with the least capability field (C_{min}). The QRREP has the design:

$$QRREP = RREP \bigcup C_{\min} \qquad (2)$$

The destination node sends a QRREP in retort to the first established QRREQ; after that only restricted QRREPs are transmitted so as to evade route reply data packets. SPRDC does not revise the QoS through route reply as the QoS does not modify considerably through this time period.

3.3.2 QoS Route Maintenance Phase

SPRDC assumes the route protection approach used in cache mechanism but with a minor alteration. When a node

comes across a serious communication problem at its MAC layer, it produces a RERR packet reverse to the source node recognizing the wrecked link. When the source node obtains a RERR packet, it eradicates the path holding wrecked link from the source node route cache. All routes that enclose the wrecked link in error are shortened at that time period. The source node then chooses a novel suitable exchange routing trail, with the highest restricted access capability (C_{min}), from the aspirant paths over which to onward any data packets along the route. When there is only a particular or no direction-finding trail accessible in the cache of the source node, then the source activates a novel route detection procedure to determine numerous partial-disjoint paths pleasing QoS constraint.

4. EXPERIMENTAL EVALUATION

Using NS2, the proposed secured QoS routing path discovery using cache mechanism [SRPDC] in wireless ad-hoc networks is configured proficiently. Every node in the network has a replicated finest effort omni-directional boundary (for cluster maintenance) with respect to a QoS supporting directional intersection. At simulation set up, all QoS associations comprise the potential to continue some of the required QoS associations, excluding formerly a QoS connection has been renowned the associated intermediary nodes may or might not enclose the bandwidth accessible to continue further QoS requests. The arrows point to gateway node and probable gateway node associations. Clusters are processed at recreation initialization. The objective is to equalize the gateway interconnections, the number of group, and the general size and difficulty in the situation tested. Once a source-destination association has been recognized, and the source commences to broadcast the data, an intermediary node is arbitrarily unconcerned. This forces the routing algorithm to both redirects the traffic from the source (FDCB) or effort to reinstate the association in the cluster connected with the detached node. In the case where the source and destination are divided only by a particular node, it is probable that the confined association reinstallation choice will be just as expensive (in terms of recovery time) as containing the source recalculate a route. As more nodes and clusters are added linking the source and destination, the restricted algorithm will exist in terms of time required to reinstate the path. The performance of the proposed secured QoS routing path discovery using cache mechanism [SRPDC] in wireless ad-hoc networks is measured in terms of

i) Routing Overhead,
ii) Average end to end delay of data packets, and
iii) Energy consumption.

Routing Overhead: Routing Overhead is the amount of routing packets broadcasted for each data packet sent in the network. For the presentation dimension, we have utilized the standardized routing weight, which is the proportion of routing packets to the data packets broadcasted.

Average End-to-End Delay of Data Packets: This is the average delay occurred among the distribution of the data packet by the source and its delivery at the analogous receiver. This comprises the entire delays basis for route acquirement, defending and dealing out at intermediary nodes, rebroadcast delays at the MAC layer, etc.

Energy consumption: The total energy required to perform the transmission over sender and receiver among the nodes in the network environment.

5. RESULTS AND DISCUSSION

Compared to an existing distributed fault tolerant quality of wireless ad-hoc networks and our previous work energy conserved fault-tolerant clusters, the proposed secured QoS routing path discovery using cache mechanism proficiently achieved the secure route path among the nodes in the network. Clustering of nodes in the network is done based on the nodes fault tolerance and mobility rate described in the pervious work. With that, in this work, we performed efficient QoS route path discovery using cache mechanism. The below table and graph describes the performance of the proposed secured QoS routing path discovery using cache mechanism [SRPDC] in wireless ad-hoc networks.

The table (Table 5.1) describes the routing overhead occurs based on the mobility rate of the nodes in the network environment. The occurrence of the routing overhead of the proposed secured QoS routing path discovery using cache mechanism is compared with an existing EFDCB (distributed fault tolerant quality of wireless ad-hoc networks) and the ECFCR (energy conserved fault-tolerant clusters with QoS routing).

Table 5.1 Mobility vs. Routing overhead

Mobility (m/s)	Routing overhead (%)		
	Proposed SRPDC	ECFCR	Existing EFDCB
10	20	22	35
20	24	27	43
30	30	33	50
40	33	40	54
50	41	45	60

60	45	50	63
70	43	55	70

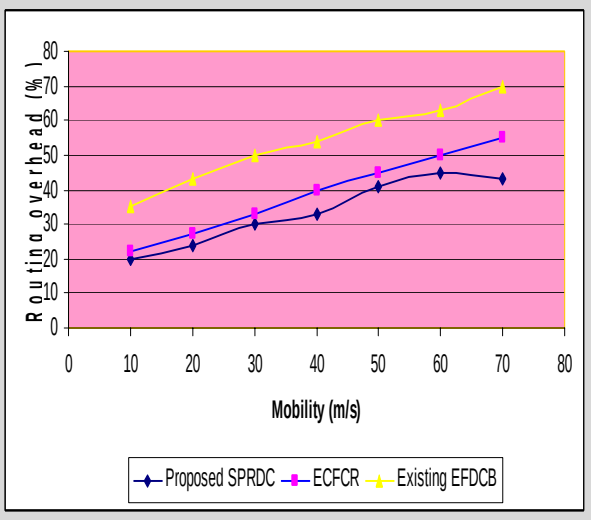

Figure 5.1 Mobility vs. Routing overhead

Figure 5.1 describes the routing overhead occurs based on the mobility rate of the nodes in the network environment. Routing Overhead is the amount of routing packets broadcasted for each data packet sent in the network. For the presentation dimension, we have utilized the standardized routing weight, which is the proportion of routing packets to the data packets broadcasted. Since the proposed SRPDC followed cache mechanism, the authenticated routing path of every node is maintained at the respective cache in the network environment. So, the occurrence of the routing overhead in the proposed SRPDC is less compared to an existing EFDCB and the ECFCR (Energy Conserved Fault-tolerant Clusters with QoS routing). Our previous work only discussed about the clustering of nodes in the network not described about the communication routing path of the nodes in the network. A cache mechanism in the proposed SPRDC maintains authenticated routing link for specific source destination pairs. The variance in the routing overhead is 40-50% less in the proposed SPRDC.

The table (table 5.2) describes the average end to end delay of packets occurred based on the traffic rate of the packets in the network environment. The occurrence of the delay of the proposed secured QoS routing path discovery using cache mechanism is compared with an existing EFDCB (distributed fault tolerant quality of wireless ad-hoc networks) and the ECFCR (energy conserved fault-tolerant clusters with QoS routing).

Table 5.2 Traffic rate vs. Average end-to-end delay of packets

Traffic rate (Kbps)	Average end-to-end delay of packets (ms)		
	Proposed SRPDC	ECFCR	Existing EFDCB
100	18	21	24
200	24	25	28
300	26	30	34
400	30	34	38
500	32	38	43
600	33	42	50
700	35	45	55

Figure 5.2 describes the average end to end delay of packets occurred based on the traffic rate of the packets in the network environment. This is the average delay occurred among the distribution of the data packet by the source and its delivery at the analogous receiver. This comprises the entire delays basis for route acquirement, defending and dealing out at intermediary nodes, rebroadcast delays at the MAC layer, etc. As the traffic rate increases in the network environment, the delay of packet delivery in the proposed SPRDC is low since it followed the cache mechanism. The cache will store all the authorized rout links from source to destination and maintained at rate of kilo bytes per second. The packet delay is measured in terms of milliseconds. The SPRDC with QoS route packet is mostly lower than the EFDCB and ECFCR because the path chosen to run the conference with SPRDC with QoS has improved bandwidth effectiveness owing to evade congestion. Compared to an existing EFDCB (distributed fault tolerant quality of wireless ad-hoc networks) and the ECFCR (energy conserved fault-tolerant clusters with QoS routing), the proposed SPRDC provides less delay in packet delivery and the variance is 35-45% low.

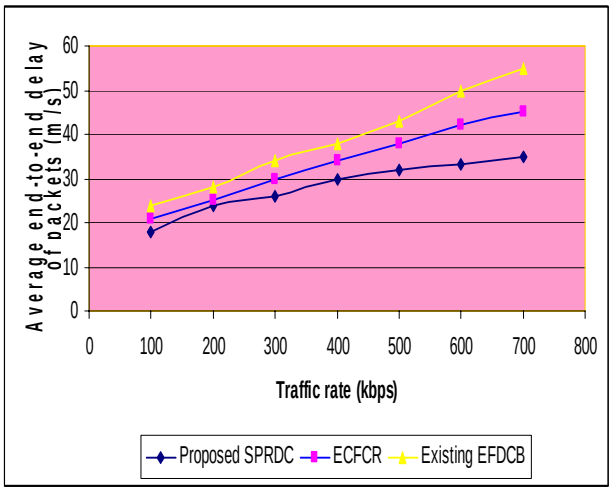

Figure 5.2 Traffic rate vs. Average end-to-end delay of packets

The table (table 5.3) describes the consumption of energy needed based on the nodes in the network environment. The energy consumption of the proposed secured QoS routing path discovery using cache mechanism is compared with an existing EFDCB (distributed fault tolerant quality of wireless ad-hoc networks) and the ECFCR (energy conserved fault-tolerant clusters with QoS routing).

Table 5.3 No. of nodes vs. Energy consumption

No. of nodes	Energy consumption (%)		
	Proposed SRPDC	ECFCR	Existing EFDCB
50	18	20	25
100	24	27	34
150	30	32	40
200	33	38	45
250	36	43	58
300	40	46	64
350	42	50	70

Figure 5.3 describes the consumption of energy needed based on the nodes in the network environment. Since the routing overhead and the packet delay is less in the proposed SPRDC, the consumption of energy is less. Since the cache mechanism is used to maintain to follow the authorized links of the route from source to destination in the nodes of the network environment. Compared to an existing EFDCB (distributed fault tolerant quality of wireless ad-hoc networks) and the ECFCR (energy conserved fault-tolerant clusters with QoS routing), the proposed SPRDC provides less consumption in energy and the variance is 40-50% low.

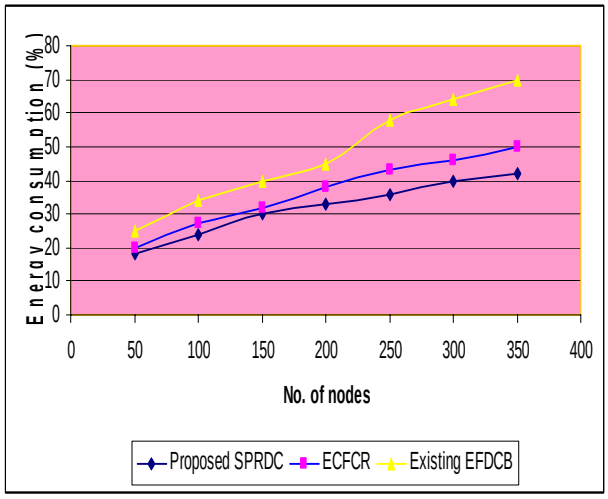

Figure 5.3 No. of nodes vs. Energy Consumption

Finally, it is being observed that the proposed secured QoS routing path discovery is efficiently achieved using cache mechanism. Link failures are guarded reliably against adversary or selfish nodes. For each node in the network environment, cache history is maintained in a secure manner which provides authenticated routing link for specific source destination pairs. Authorized nodes in the ad hoc network delineate the inappropriate routing directions.

6. CONCLUSION

The work presented secured QoS routing path discovery is efficiently achieved using cache mechanism to enhance an effective communication of the nodes in the network. Clustering is done effectively in the previous work based on node's fault tolerance rate, energy consumption and mobility rate. Routing security is done efficiently using cache mechanism to evade misdirecting malicious node. Link failures are guarded reliably against adversary or selfish nodes. For each node in the network, cache history is maintained which provides authenticated routing link for specific source destination pairs. Authorized nodes in the ad hoc network delineate the inappropriate routing directions. This cache mechnaims enhanced the QoS routing path based on mobile node preferences and minimizes the communication overhead. It progress the QoS routing path in wireless ad hoc network on preferential QoS metrics which decrease packet delay, and the energy consumption. An experimental evaluation has shown that the proposed Secured QoS Routing Path Discovery using Cache mechanism [SRPDC] in wireless ad-hoc networks provides an efficient secure route path discovery to progress an efficient node communication among the nodes in the network environment.

REFERENCES

[1] Ananda Krishna B et. Al., "Improving Quality of Service Through Secured Routing In Mobile Ad Hoc Networks", Int. J.Advanced Networking and Applications Volume: 03, Issue: 04, Pages:1253-1260 (2012)

[2] D.Srinivasa Rao et. Al., "Detection of Routing Anomaly using IDS Architecture based on Agents and Clusters in MANETs", International Journal of Computer Applications (0975 – 8887), Volume 26– No.4,July 2011.

[3] M.K. Nakayama, "Statistical analysis of simulation output", Proc. Winter Simulation Conference, 2008, pp. 62–72.

[4] I.D. Chakeres, E.M. Belding-Royer, J.P. Macker, "Perceptive Admission Control for Wireless Network Quality of Service", *Elsevier Ad hoc Networks*, Vol. 5, No. 7, September 2007, pp. 1129–1148.

[5] Haseeb Zafar et. Al., " QoS-aware Multipath Routing Scheme for Mobile Ad Hoc Networks", International Journal of Communication Networks and Information Security (IJCNIS) Vol. 4, No. 1,April 2012

[6] E. Çayırcı and C. Rong, "Routing in Ad Hoc Sensor and Mesh Networks", in Book Security in Wireless Ad Hoc and Sensor Networks (chapter 5), CRC Press LLC, 2009.

[7] K. Kumar, "Intrusion Detection in Mobile Ad hoc Networks," Master's Thesis, University of Toledo, December 2009.

[8] E. Çayırcı and C. Rong, "Security Attacks in Ad Hoc, Sensor and Mesh Networks," Security in Wireless Ad Hoc and Sensor Networks (Chapter8), CRC Press LLC, 2009.

[9] H. Zafar, D. Harle, I. Andonovic, Y. Khawaja,"Performance Evaluation of Shortest Multipath Source Routing cheme", *IET Communications,* Vol. 3, No. 5, May 2009, pp. 700–713.

[10] Q. Chen, et. Al., "Overhaul of IEEE 802.11 modelling and simulation in ns-2", Proc. 10th ACM Symposium on Modelling, Analysis, and Simulation of Wireless and Mobile Systems, Chania, Greece, October 2007.pp. 159–168.

[11] R.D. Renesse, V. Friderikos, H. Aghvami, "Cross-Layer Cooperation for Accurate Admission Control Decisions in Mobile Ad Hoc Networks", *IET Communications*, Vol. 1, No. 4, August 2007, pp. 577–586.

[12] R.S. Chang, C.F. Lin, "Using Link Layer Throughput Maximization in Ad Hoc Network Routing Algorithms", *IET Communications*, Vol. 1, No. 5, October 2007, pp. 875–879.

AUTHOURS PROFILE

Dr.P.Thangaraj received the Bachelor of Science degree in Mathematics from Madras University in 1981 and his Master of Science degree in Mathematics from the Madras University in 1983. He completed his M.Phil degree in the year 1993 from Bharathiyar University. He completed his research work on Fuzzy Metric Spaces and awarded Ph.D degree by Bharathiyar University in the year 2004. He completed the post graduation in Computer Applications at IGNOU in 2005. His thesis was on "Efficient search tool for job portals". He completed his Master of Engineering degree in Computer Science in the year 2007 from Vinayaka Missions University. His thesis was on "Congestion control mechanism for wired networks". Currently he is a Professor and Head of Computer Science and Engineering at Bannari Amman Institute of Technology, Sathyamangalam. His current area of research interests are in Fuzzy based routing techniques in Ad-hoc Networks.

A. M.Renuka received the Bachelor of Science degree in Computer Science from Madras University in 1999 and her Master degree in Computer Application from the Bharathidasan University in 2002. She completed her M.Phil degree in the year 2005 from Periyar University. She is pursuing Ph.D.,in Computer Science at Mother Teresa University. Currently working as a Assistant Professor in the Department of Applied Science at SSM College of Engineering, Komarapalayam. She is presently working in the area of Mobile Security. Other areas of interest include Design and Analysis of Algorithms, Software Engineering and Extreme Programming.

Dr.S.N.Sivanandam completed his B.E. (Electrical Engineering) in 1964 from Government College of Technology, Coimbatore, and MSc (Engineering) in Power Systems in the year 1966 from PSG College of Technology, Coimbatore. He acquired PhD in control systems in 1982 from Madras University. He received best teacher award in the year 2001 and **Dhakshina Murthy Award** for teaching excellence from PSG College of technology. He received the citation for best teaching and technical contribution in the year 2002, Government College of Technology, Coimbatore. His research areas include Modeling and Simulation, Neural Networks, Fuzzy Systems and Genetic Algorithm, Pattern Recognition, Multidimensional system analysis, Linear and Non linear control system, Signal and Image processing, Control System, Power System, Numerical methods, Parallel Computing, Data Mining and Database Security. He is a member of various professional bodies like IE (India), ISTE, CSI, ACS and SSI. He is a technical advisor for various reputed industries and engineering institutions.