AN APPROACH FOR SECURE ENERGY EFFICIENT ROUTING IN MANET

Nithya.S[1] and Chandrasekar.P[2]

[1]II ME (CS), Sri Shakthi Institute Of Engineering and Technology,
Anna University of Technology, Coimbatore, India
[2] Assistant Professor(S) ECE, Sri Shakthi Institute of Engineering and Technology,
Anna University of Technology, Coimbatore, India

ABSTRACT

MANET is a network, which is very popular due to its unique characteristics from all the other types of networks. MANET is a network having tiny light weighted nodes, with no clock synchronization mechanisms. The wireless and distributed nature of MANETs poses a great challenge to system energy and the security. Generally, in this type of network the exhaustion of energy will be more and as well, the security is missing due to its infrastructure less nature. Due to the lack of energy, the node not only affect the node itself but also it affects its ability to forward packets on behalf of others and thus it affects its overall network lifetime. Similarly, the node causes cheating during the transmission process in the network due to network overloading. Most MANET routing protocols are vulnerable to attacks that can freeze the whole network. Thus these may affects the performance of the network. To overcome these problems, we propose a new secured energy efficient routing algorithm namely called SRMECR. This algorithm holds two mechanisms. Initially it makes all the active state nodes to sleep when not in use, and then finds the efficient path for reliable data transmission. They minimize either the active communication energy required to transmit or receive packets or the inactive energy consumed when a mobile node stays idle but listens to the wireless medium for any possible communication requests from other nodes. Secondly, provides the security against routing reply attacks. By simulation based studies, we show that this algorithm effectively provides higher security with less energy consumption.

KEYWORDS**:** *Energy, Link failure, MANET, Network, Security.*

I. INTRODUCTION

Mobile devices coupled with wireless network interfaces will become an essential part of future computing environment consisting of infra-structured and infrastructure-less mobile networks. Wireless local area network based on IEEE 802.11 technology is the most prevalent infra-structured mobile network, where a mobile node communicates with a fixed base station, and thus a wireless link is limited to one hop between the node and the base station. Mobile ad hoc network (MANET) is an infrastructure-less multi hop network where each node communicates with other nodes directly or indirectly through intermediate nodes. Thus, all nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes. Since MANETs are self-organizing, rapidly deployable wireless networks, they are highly suitable for applications involving special outdoor events, communications in regions with no wireless infrastructure, emergencies and natural disasters, and military operations. Routing is one of the key issues in MANETs due to their highly dynamic and distributed nature. In particular, energy efficient routing may be the most important design criteria for MANETs since mobile nodes will be powered by

batteries with limited capacity. Power failure of a mobile node not only affect the node itself but also its ability to forward packets on behalf of others and thus the overall network lifetime. The performance of a mobile ad hoc network mainly depends on the routing scheme.

Our critical issue for almost all kinds of portable devices supported by battery power is power saving. Routing is one of the key issues in MANET due to its highly dynamic and distributed nature. Without power, any mobile device will become useless. Battery power is a limited resource, and it is expected that battery technology is not likely to progress. Hence lengthen the lifetime of the batteries is an important issue, especially for MANET, which is all supported by batteries [1],[2],[3].

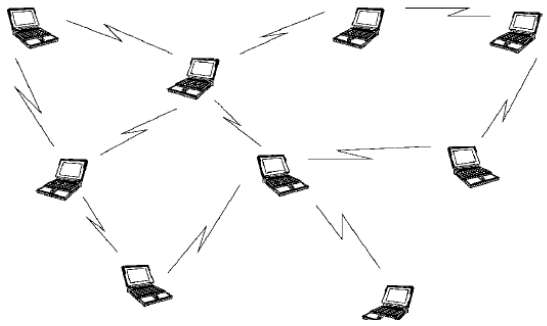

Fig 1: Ad Hoc Network Architecture

The previous energy-efficient algorithms can try to reduce the energy consumption. However while considering minimum energy path, they do not considering the reliability of the links. This may result in low quality of service, less reliable path. When we consider the reliability of the network, energy consumption of the network will be high. Similarly, Security is a more sensitive issue in MANETs than any other networks due to lack of infrastructure and the broadcast nature of the network. The nature of ad hoc networks poses a great challenge to system security designers due to the following reasons: Firstly, wireless network is more susceptible to attacks ranging from passive eavesdropping to active interfering, Trusted Third Party adds the difficulty to deploy security mechanisms, mobile devices tend to have limited power consumption and computation capabilities, finally, node mobility enforces frequent networking reconfiguration which creates more chances for attacks. [4], [5].

There are five main security services for MANETs: authentication, confidentiality, integrity, non-repudiation, availability. Among all the security services, authentication is probably the most complex and important issue in MANETs. Several security protocols have been proposed for MANETs, there is no approach fitting all networks, because the nodes can vary between any devices. In order to overcome these problems, we propose a new secured energy efficient routing algorithm.

The main contribution of this paper is in showing how power aware routing must not only be based on node specific parameters (e.g. residual battery energy of the node), but must also consider the link specific parameters (e.g. channel characteristics of the link) as well, to increase the operational lifetime of the network. And also provides the security against route reply attacks using a check sum mechanism. It may also balance the traffic load in the network, while finding the reliable transmission path. Sleep/Active mode approach and Transmission Power Control Schemes are the main two methodologies, which are mainly responsible for considerable energy saving. The rest of the paper is organized as follows: In Section II, we provide an overview of the prior energy-aware routing algorithms in our own words. Then in Section III, we explain the SRMECR routing algorithm. In Section IV, we present the simulation results, and we conclude our work in Section V.

II. AN OVERVIEW OF RELATED WORK

Mobile ad hoc network (MANET) is an infrastructure-less multi hop network where each node communicates with other nodes directly or indirectly through intermediate nodes. Thus, all nodes in a MANET basically function as mobile routers participating in some routing protocol required for deciding and maintaining the routes. Among the various network architectures, design of the mobile ad hoc networks (MANET) plays an important role. Such a network can either operate in a standalone fashion with the ability of self-configuration and no clock synchronization mechanism. Mobile Ad-hoc

networks are self-organizing and self-configuring multi-hop wireless networks where, the structure of the network changes dynamically. No base stations are supported in such an environment, and mobile hosts may have to communicate with each other in a multi-hop fashion. Minimal configuration and fast deployment make MANETs suitable for emergency situations like natural or human-induced disasters and military conflicts. Mobile devices coupled with wireless network interfaces will become an essential part of future computing environment consisting of infra-structured and infrastructure-less mobile networks.

Energy management in wireless networks is very important due to the limited energy availability in the wireless devices. It is important to minimize the energy costs for communication as much as possible by practicing energy aware routing strategies. Based on the observations of signal attenuations, many routing protocols are operated. Energy aware routing algorithm would select a route comprising multiple short distance hops over another one with a smaller hop count but larger hop distances. The PAMAS (Power aware Multi access protocol with signaling) [6] protocol allows a host to power its radio off when it has no packet to transmit/receive or any of its neighbors is receiving packets, but a separate signaling channel to query neighboring hosts' states is needed. In PAMAS, [7] they provide several sleep patterns and it allows the mobile nodes to select their sleep patterns based on their battery power. But this needs a special hardware called RAS (Remote Activated Switch). But they biased towards smaller hops typically led to the selection of paths with a very large hop count.

The PARO [7], [8] has proposed for the situation where the networks having the variable transmission energy. This protocol essentially allows an intermediate node to insert itself in the routing path if it detects potential savings in the transmission energy. Later, Connected-dominated set based power saving protocol is proposed. In which some hosts must as a coordinators, which are chosen according to their remaining battery energies and the numbers of neighbors they can connect .In this type of network, only coordinators need to awake, other hosts can enter the sleeping mode.

Min-Hop routing is the conventional "energy unaware" routing algorithm, where each link is assigned based on the identical cost. In which it simply selects the routes based upon the number of hops. Less number of hop counts path is considered as a route for transmission of packets. Thus results in less reliability and power wastage. Min Energy routing is another power aware routing algorithm, which simply selects the path corresponding to the minimum packet transmission energy for reliable communication, without considering the battery power of individual nodes. In which the number of hops and delay increases. This results in less energy consumption but with less reliability

The MTPR mechanism uses a simple energy metric, represented by the total energy consumed to forward the information along the route. This way, MTPR reduces the overall transmission power consumed per packet, but it does not affect directly the lifetime of each node (because it does not take account of the available energy of network nodes). Notice that, in a fixed transmission power context, this metric corresponds to a Shortest Path routing.

Huaizhi Li and Mukesh Singhal [9] have presented an on-demand secure routing protocol for ad hoc networks based on a distributed authentication mechanism. The protocol has made use of recommendation and trust evaluation to establish a trust relationship between network entities and it uses feedback to adjust it. The protocol does not need the support of a trusted third party and it discovers multiple routes between two nodes. Sec AODV [10] is the one of the protocol that incorporates security features of non-repudiation and authentication, without relying on the availability of a Certificate Authority (CA) or a Key Distribution Center (KDC). They have presented the design and implementation details of their system, the practical considerations involved, and how these mechanisms are used to detect and thwart malicious attacks. Packet conservation Monitoring Algorithm (PCMA) [11] can be used to detect selfish nodes in MANETs. Though the protocol addresses the issue of packet forwarding attacks, it does not address other threats.

Syed Rehan Afzal et al. [12] have explore the security problems and attacks in existing routing protocols and then they have presented the design and analysis of a secure on-demand routing protocol, called RSRP which has confiscated the problems mentioned in the existing protocols. Moreover, unlike Ariadne, RSRP has used a very efficient broadcast authentication mechanism which does not require any clock synchronization and facilitates instant authentication.

III. SRMECR ALGORITHM

A mobile node consumes its battery energy not only when it actively sends or receives packets but also when it stays idle listening to the wireless medium for any possible communication requests from other nodes. Thus, energy efficient routing protocols minimize either the active communication energy required to transmit and receive data packets or the energy during inactive periods. Secondly, Security is a more sensitive issue in MANETs than any other networks due to lack of infrastructure and the broadcast nature of the network. While MANETs can be quickly set up as needed, they also need secure routing protocols to add the security feature to normal routing protocols. The need for more effective security measures arises as many passive and active security attacks can be launched from the outside by malicious hosts or from the inside by compromised nodes. Key management is a fundamental part of secure routing protocols; existence of an effective key management framework is also paramount for secure routing protocols. Several security protocols have been proposed for MANETs, there is no approach fitting all networks, because the nodes can vary between any devices. Our newly proposed secure energy aware algorithm holds two mechanisms.

3.1 Efficient Node Selection mechanism:

This mechanism deals with the reduction of energy consumption. It makes all the active state nodes to sleep when not in use by means of active sleep state methodology. This Active /sleep state methodology initially categorize the energy as active communication energy and inactive communication energy. The active communication energy was reduced by adjusting the power of the each node to reach only the particular destination and not more than that. The inactive communication energy was reduced by simply turns off the node during the idle case.

This leads to considerable energy savings, especially when the network environment is characterized with low duty cycle of communication activities. Secondly, it will find the route with least cost path based on the reliability and the residual battery energy. This algorithm assumes RREQ (Repeat Request) for reliable packet transmission in each hop. If the packet or its acknowledgement is lost, the sender will retransmit the packet. To formulate this algorithm, assume E be the energy expected by the node to transmit the packets from source to destination.

E (i, j) -> Expected Energy to Transmit a Packet

B (i) -> Total Residual Battery Energy

R= B-E-> Remaining Residual Battery Energy

The ratio of the fraction of residual battery energy to be consumed to the total residual battery energy (B) gives the link weight. The path with less weight is to be selected. The Link weight is defined as the fraction of the residual battery energy that node i consumes to transmit a packet reliably over (i, j). Link weight is determined using Dijkstra's algorithm.

Link Weight= E (i, j)/B (i)

If the residual energy of the nodes is not considered, then the energy in the best path's node will be consumed more than the other nodes in the network. In this model the consumed energy by a node during packet transmission consists of two elements. The first element is the energy consumed by the processing part of the transceiver circuit, and the second element is the energy consumed by the transmitter amplifier to generate the required power for signal transmission.

3.2 Transmission Power Control Mechanism:

In Ad-hoc network, the packets are transmitted with minimum power, which is required for decoding the packets. In such a situation, TPC (Transmission Power Control) scheme is used. This transmission power control approach can be extended to determine the optimal routing path that minimizes the total transmission energy required to deliver data packets to the destination.

In wireless communication transmission power has strong impact on bit error rate, and the inter radio interference. Thus this transmission power control scheme which will adjust the transmission power of the node based on the link distance. If TPC is not present, then the maximum transmission power is utilized. If the residual energy of the nodes is not considered, then the energy in the best path's node will be used more unfairly than the other nodes in the network. Because of their battery depletion, these

nodes may fail after a short time, whereas other nodes in the network may still have high energy in their batteries.

3.3 Secure Route Discover Process:

This mechanism deals with the security aspects. In order to make our proposed algorithm more secure, a new cryptographic check sum mechanism is used. The proposed algorithm is very effective as it detects the malicious node quickly and it provides security against the attacks. Among all the security services, authentication is probably the most complex and important issue in MANETs. Cryptographic mechanisms make use of a hash code. Hash code does not use a key but is a function only of the input message. The message plus concatenated hash code is encrypted using symmetric encryption.
In this proposed algorithm, initially once a node S want to send a packet to a destination node D, it initiates the route discovery process by constructing a route request RREQ packet. It contains the source and destination ids and a request id. When an intermediate node receives the RREQ packet for the first time, it appends its id to the list of node ids and signs it with a key which is shared with the destination. It then forwards the RREQ to its neighbors. When the destination receives the accumulated RREQ message, it first verifies the sender's request id by recomputing the sender's MAC value, with its shared key. It then verifies the digital signature of each intermediate node. If all these verifications are successful, then the destination generates a route reply message RREP. If the verifications fail, then the RREQ is discarded by the destination. It again constructs a MAC on the request id with the key shared by the sender and the destination.

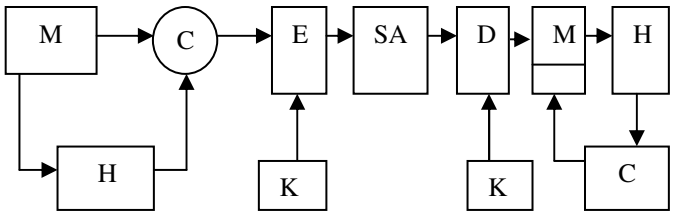

Fig 2: Basic Security Function

M-Message
H-Hash Code
C-Concatenation
E-Encryption
SA- Secure Message
D-Decryption
K-Secret Key
COMP-Comparison
Secondly the figure indicates that, the message and the hash function are concatenated. Then the concatenated hash code along with the message is encrypted using symmetric key encryption. The bank block indicates the encrypted value of concatenated hash code with message. The Message must be transferred only between the source and the destination using the secret key, thus the data transmission is more secure and has not been altered. The comparative block predicts the absolute key value with secured message. The hash code provides the structure or redundancy required to achieve authentication. Because encryption is applied to the entire message plus hash code, Confidentiality is also provided. If in the case of many intermediate states present between the source and the destination, then the security is achieved by means of digital signatures. Thus, our new secure energy aware algorithm with these two mechanisms enhances the routing problem and manages the network resources of achieving fair resources usage across the network node with higher security.

IV. PERFORMANCE EVALUATION

4.1Simulation model:

Consider an ad hoc network in which nodes are uniformly distributed in a square area. In the network, sessions are generated between randomly chosen source-destination nodes with exponentially

distributed inter-arrival time. The source node of the session transmits data packets with the constant rate 1 packet/sec. We developed our simulation model using ns 2.34 simulator. The ns 2.34 simulator allows extracting from a simulation many interesting parameters, like throughput, data packet delivery ratio, end-to-end delay and overhead, [16].
To have detailed energy-related information over a simulation, we modified the ns 2.34 simulator code to obtain the amount of energy consumed over time by type (energy spent in transmitting, receiving, overhearing or in idle state), [17]. This way, we obtained accurate information about energy at every simulation time. We used these data to evaluate the protocols from the energetic point of view: we will see the impact of each protocol on different new parameters, like the number of nodes alive over time (to check the lifetime of nodes), the expiration time of connections (to see the network lifetime), and the energy usage divided by type (receiving, transmitting, overhearing).

4.1.1 Practical Considerations:

The routing protocols for MANET'S are generally categorized as table driven, and on demand driven based on the timing of when the routes are updated. SRMECR algorithm can be implemented with the existing routing protocols for ad hoc networks. Here, we implemented with AODV as the routing protocol. The algorithm performance was compared with the normal AODV protocol. An AODV is an on demand routing protocol that combines the capabilities of both DSR and DSDV protocol. It uses route discovery and route maintenance from DSR and in addition to the hop by hop routing sequence numbers and periodic beacons from Destination-Sequenced Distance vector (DSDV) routing protocol. AODV is an on demand routing protocol in which routes are discovered only when a source node desires them. Route discovery and route maintenance are two main procedures: The route discovery process involves sending route-request packets from a source to its neighbor nodes, which then forward the request to their neighbors, and so on. Once the route-request reaches the destination node, it responds by uni casting a route-reply packet back to the source node via the neighbor from which it first received the route request. When the route-request reaches an intermediate node that has a sufficiently up-to-date route, it stops forwarding and sends a route-reply message back to the source. Once the route is established, some form of route maintenance process maintains it in each node's internal data structure called a route-cache until the destination becomes inaccessible along the route. Note that each node learns the routing paths as time passes not only as a source or an intermediate node but also as an overhearing neighbor node.

Table1: Simulation Parameters

Area Size	1000 X 1000
Simulation time	400 s
Number of Nodes	11
MAC type	MAC 802.11
Traffic Source	CBR
Initial Energy	1000 J
Packet Size	512 Bytes
Routing Protocol	AODV
Nodes Speed	3 m/s
Beacon Period	200 ms

4.1.2 Simulation Results

The following results show the operation of new secure energy aware algorithm. Some parameters like packets received, Energy consumption per packet transmission, end to end latency and packet delivery ratio Throughput are analyzed to verify the performance of the new power aware mechanisms. As dealing with the energy and security aspect, our model AODV protocol was compared with other existing protocols such as RSVP and SAODV Protocol. Our New model AODV (Secure Energy aware Mechanism) shows good energy efficiency when compared with the all other existing protocols.

Energy Consumption per packet:

It defines the energy consumed by a node to transmit a packet from source to destination. In the below graph we compared the plain AODV protocol with our new secure energy aware mechanism. By means of new secure energy aware mechanism the power consumed by the node to transmit to the packet was decreased at a higher rate. The energy consumption per packet was decreased as previous. This will highly increases the network life time.

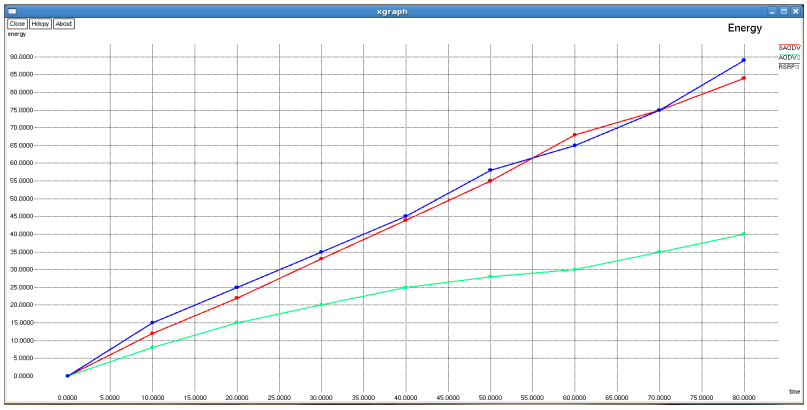

Fig 3: Energy Consumption per Packet

Packet delivery ratio:

Data packet delivery ratio can be calculated as the ratio between the number of data packets that are sent by the source and the number of data packets that are received by the sink. This is the amount of successful received bits at the destination nodes for the entire simulation period. Packet delivery ratio should be always high for the efficient algorithm or a protocol. The figure 4 shows the packet delivery ratio was high when compared with the previous methodology.

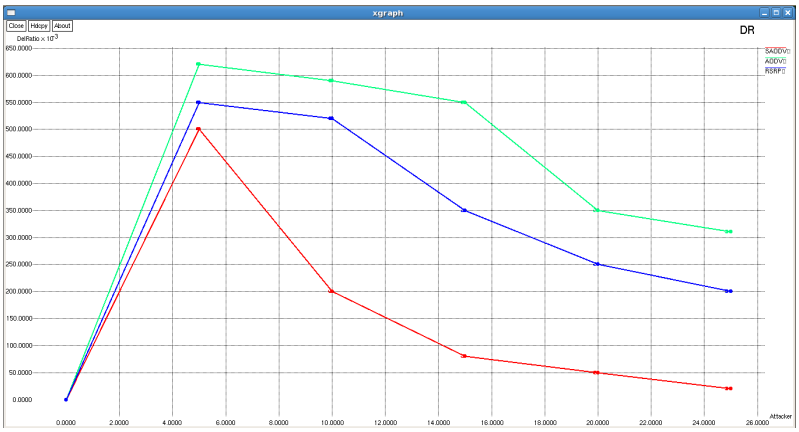

Fig 4: Packet delivery ratio

End To End Latency:

End-to-end Latency refers to the time taken for a packet to be transmitted across a network from source to destination.End to end latency which includes all possible delays caused by buffering during route discovery time, queuing at the interface queue, retransmission, and processing time. It defines the ratio of interval between the first and the second packets to a total packets delivery. This figure 5 shows the result of end to end latency.

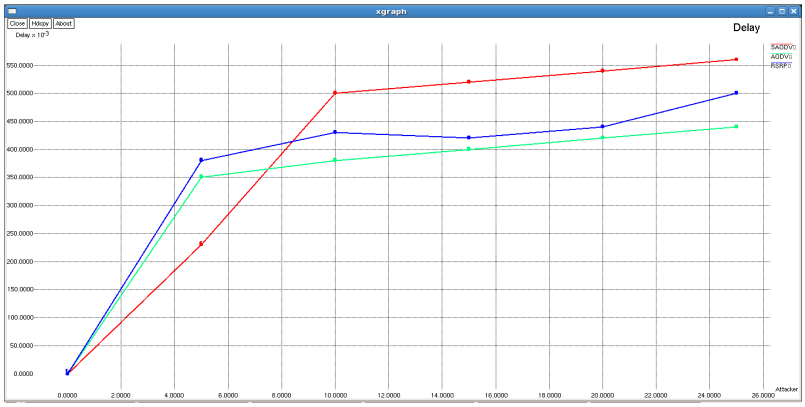

Fig 5: End To End Latency

The end to end latency of the new secure energy aware mechanism was highly reduced when compared with normal protocol operations.

Overhead:

The control overhead is defined as the total number of routing control packets normalized by the total number of received data packets. When compared with the other existing protocols, our mechanisms hold less number of overhead packets.

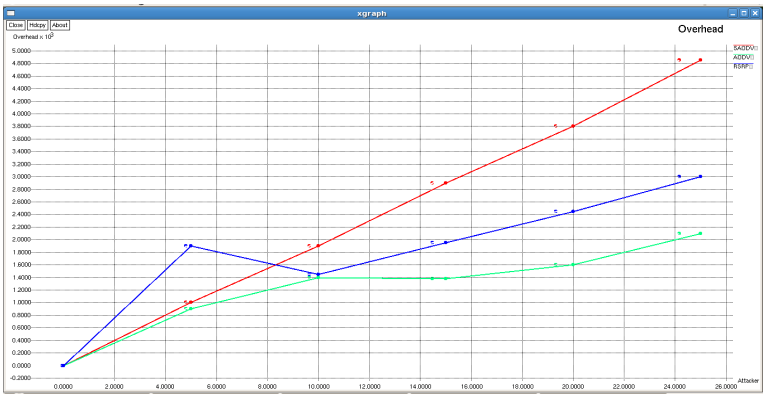

Fig 6: Overhead

Throughput:

Throughput is defined as the total amount of data packets delivered at the destination from the source without an error. By means of using this new secure energy aware mechanism, the higher amount of data's was received at the destination without an error. Thus the figure 6 shows that our algorithm provides higher throughput than the other existing protocols.

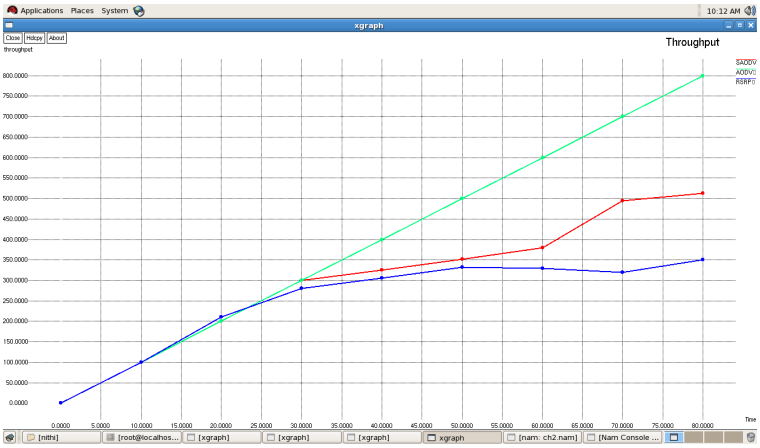

Fig 6: Throughput

V. CONCLUSION

In this paper, a new secure energy aware routing SRMECR algorithm was proposed. It mainly defines the least cost path based on the reliability and the remaining energy of the node for packet transmission from, source to destination, and making the sleep/active state methodology for providing the energy efficiency. Later this algorithm provides a new cryptographic check sum mechanism to prevent the communications from attackers. By means of these features, we may effectively secure our data's with minimal energy consumption Thus; this algorithm can effectively reduce the energy consumed by the node as well as increases the security and reliability of the network. This in turn increases the operational lifetime and it maintains the load traffic as well.

REFERENCES

[1].X.-Y. Li, Y. Wang, H. Chen, X. Chu, Y. Wu, and Y. Qi, "Reliable and energy-efficient routing for static wireless ad hoc networks with unreliable links," IEEE Trans. Parallel Distrib. Syst., vol. 20, no. 10, pp. 1408–1421, 2009.

[2]. B. Mohanoor, S. Radhakrishnan, and V. Sarangan, "Online energy aware routing in wireless networks," Ad Hoc Networks, vol. 7, no. 5, pp. 918–931, July 2009.

[3].Ashwani kush ,Divya Sharma, Sunil Taneja, "A Secure and Power Efficient Routing Scheme for Ad Hoc Networks", International journal of Computer Applications, Volume 21-No 6, May 2011

[4].V. Kanakaris*, D. Ndzi and D. Azzi., Ad-hoc Networks Energy Consumption: A review of the Adhoc Routing Protocols, Journal of Engineering Science and Technology Review 3 (1) (July 2010).

[5].Dr. A. Rajaram, J. Sugesh, Power Aware Routing for MANET using on Demand Multi path Routing Protocol, International Journal of Computer Science Issues, Vol. 8, Issue 4, No 2, July 2011.

[6].Dhiraj Nitnaware1 & Ajay Verma, "Performance Evaluation of Energy Consumption of Reactive Protocols under Self-Similar Traffic", International Journal of computer science and communication vol.1, No.1, January-June 2010.

[7] Busola S.Olagbegi and Natarajan Meganathan "A Review Of the Energy Efficient and Secure Multicast routing protocols for mobile ad hoc networks", International journal on applications of graph theory in wireless ad hoc networks and sensor networks,Vol 2, No.2, June 2010

[8].J. Gomez, A. T. Campbell, M. Naghshineh, and C. Bisdikian, "Paro: supporting dynamic power controlled routing in wireless ad hoc networks," Wireless Networks, vol. 9, no. 5, pp. 443–460, 2003.

[9]. Huaizhi Li and Mukesh Singhal, 2006."A Secure Routing Protocol for Wireless Ad Hoc Networks", in proceedings of *39th Annual Hawaii International Conference on System Sciences*, Vol.9.

[10]. A. Patwardhan, J. Parker, M. Iorga, A. Joshi, T. Karygiannis and Y. Yesha, 2008. "Thresholdbased intrusion detection in ad hoc networks and secure AODV", Vol.6, No.4, pp.578-599.

[11]. Tarag Fahad & Robert Askwith, 2006. "A NodebMisbehaviour Detection Mechanism forbMobile Ad-hoc Networks" The *7th Annual PostGraduate Symposium on the Convergence of Telecommunications, Networking and Broadcasting*.

[12]. M. Mohammed, Energy Efficient Location Aided Routing Protocol for Wireless MANETs, International Journal of Computer Science and Information Security, vol. 4, no. 1 & 2, 2009.

[13].J. Vazifehdan, R. Hekmat, R. V. Prasad, and I. Niemegeers, "Performance evaluation of power-aware routing algorithms in personal networks," in *The 28th IEEE International Performance Computing and Communications Conference (IPCCC '09)*, pp. 95–102, Dec. 2009.
[14].Wang Yu, "Study on Energy Conservation in MANET", Journal of Networks, Vol. 5, No. 6,June 2010.
[15].Niranjan Kumar Ray & Ashok Kumar Turuk, (2010) "Energy Efficient Techniques for Wireless Ad Hoc Network", *International Joint Conference on Information and Communication Technology*,pp105-111.
[16]. Ns-2 network simulator, http://www.isi.edu/nsnam/ns/, 1998.
[17]. Marc Greis' Tutorial for the UCB/LBNL/VINT Network Simulator "ns".

Authors

Nithya.S is doing ME Communication systems in Sri Shakthi Institute of Engineering & Technology, Coimbatore. She has done her BE in ECE from Sengunthar Engineering college, Tiruchengode, Tamil Nadu. Her research interests include mobile adhoc networks. She has presented 2 papers in international conference. She has published 1 paper in international journal.

Chandra Sekar.P is with the ECE department in Sri Shakthi Institute of Engineering &Technology, Coimbatore as Assistant professor(S). He has done his B.E in Electronics & Communication Engineering from Jayam College of Engg. And Tech.,Dharmapuri, Tamilnadu, M.E.in Network Engineering from Arulmigu Kalasalingam College of Engineering Srivalliputur,Tamilnadu and pursuing PhD under Anna University of Technology, Coimbatore. His research interest is Routing in MANET. He has 10 years of experience in teaching. He has presented 4 papers in national conference and 5 papers in international conferences. He has published 3 papers in international journal.