A New Approach of Secure Power Aware Routing for Mobile Ad-Hoc Network

Manesh P. Patil
Department of Computer Engineering
S.S.V.P.S's B.S.Deore College of Engineering, Dhule. (M.H.), India

ABSTRACT

In order to assist communication within a mobile Ad-Hoc network, a well-organized routing protocol is required to determine routes between mobile nodes. Power is one of the most important design criteria for Ad-Hoc networks as batteries provide inadequate working capacity to the mobile nodes. Power failure of a mobile node not only affects the node itself but also its ability to forward packets on behalf of others and hence affects the overall network lifetime. Much research efforts have been devoted to develop energy aware routing protocols. In this paper we propose an efficient algorithm, which maximizes the network lifetime by minimizing the power consumption during the source to destination route establishment alongside making the node secure. Limited resource availability such as battery power and security are the major issues to be handled with mobile Ad-Hoc networks. By using Efficient secure routing protocol for mobile ad hoc networks that achieves secrecy of data message and secure the routing operation. The security schemes aims at preventing attacks by malicious node that intentionally disrupt the route discovery process. The protocol also assures a source node generates a route discovery request is able to identify and authenticate the route reply from destination. In mobile Ad-Hoc networks, an attacker can easily disrupt the functioning of the network by attacking the underlying routing protocol. Packets are secure during source to destination transmission by using Two Fish Encryption algorithm. As a case study proposed algorithm has been incorporated along with the route discovery procedure of AODV and PAR, by simulation it is observed that proposed algorithm's performance is better as compare to AODV and PAR in terms of packet delivery ratio and network lifetime for different network scenarios.

Keywords

Ad-Hoc networks, Power Aware Routing, Secure Power Aware Routing Protocol, and Ad-Hoc on Demand Distance Vector Protocol, Mobile Ad-Hoc Network, AODV, MANET and Two-fish.

1. INTRODUCTION

A mobile Ad-Hoc network (MANET) [1] is an autonomous system of mobile nodes (and associated hosts) connected by wireless links. Mobile Ad-Hoc Network (MANET) is a wireless network without any fixed infrastructure or centralized control; it contains mobile nodes that are connected dynamically in an arbitrary manner. Based on infrastructure, the wireless networks broadly classified into two types, first type infrastructure networks contains Base stations. The second type is called Mobile Ad-Hoc Networks enable users to communicate without any physical infrastructure regardless of their geographical location. Each node operates not only as an end-system, but also as a node to forward the packets. The nodes are free to move about and organize themselves into a network. The main application of mobile Ad-Hoc network is in emergency rescue operations and battlefields. This paper addresses the problem of secure power awareness routing to increase lifetime of overall network. Since nodes in mobile Ad-Hoc network can move randomly, the topology may change arbitrarily and frequently at unpredictable times. Transmission and reception parameters may also impact the topology. Therefore it is very difficult to find and maintain an optimal power aware route. In general the main security requirements for any system will be confidentiality, authentication, integrity, non-repudiation, availability, and access control. Confidentiality ensures that eavesdroppers will not be able to read the information sent through the network which may be achieved by encrypting data and control packets. Authentication prevents impersonation and verifies the identity of the nodes. Integrity will insure that packets will not be modified or altered by an adversary [2]. The main aim of proposed routing is to increase the life time of network with low overhead while achieving many desired features of routing protocol of MANET. It selects the optimal paths using power aware metric and optimizes the power consumption, overhead and bandwidth. It supports reliability by providing node- disjoint paths and it provides the stability (increasing mean life time of the nodes) by distributing the burden of routing and congestion control [3]. Propose a Trust-Aware Routing Protocol (TARP) for secure-trusted Ad-hoc routing. In TARP security is inherently built into the routing protocol where each node evaluates the trust level of its neighbors based on a set of attributes. TARP is based on three new concepts. First, for route establishment, a new secure ad-hoc routing mechanism is used second six security parameters considered in computing the trust-level of a node in a given route and include: software configuration, hardware configuration, battery power, credit history, exposure and organizational hierarchy [4]. Security is a critical issue in an ad hoc network. In this investigate by simulation the performance of the SPREAD scheme that we proposed as a complementary mechanism to enhance the data confidentiality service in an ad hoc network. The SPREAD scheme is based on the idea to distribute a secret among multiple independent paths while it is transmitted across the network. Through simulation, the effectiveness of SPREAD in improving network security is verified [5]. The implementation and testing of a new power-aware algorithm, PSWA, associated with a Cache System, and tested with the WRP routing protocol, in a Mobile Ad hoc Network scenario. A scheme that does not use the sleep schedule for the nodes it was used; nodes automatically fall asleep if they do not deal with data and routes [6]. In this work a scheme has been proposed to maximize the network lifetime and minimizes the power consumption during the source to destination route establishment. Also by using route selection criteria trusted nodes are. Proposed work is aimed to provide efficient real and non real time data transfer. Rest of the paper is organized as follows: Section 2 discusses the study on the related work. In section 3 working of the proposed secure power aware

routing (SPAR) scheme have been given in detail. Section 4 discusses the Two-Fish Encryption Algorithm. Section 5 simulation framework and results and Section 6 concludes the paper.

2. RELATED WORK

Many research efforts have been devoted for developing secure power aware routing protocols. Different approaches can be applied to achieve the target [7]. Transmission power control and load distribution are two approaches to minimize the active communication energy, and sleep/power-down mode is used to minimize energy during inactivity. The primary focus of the above two approaches is to minimize energy consumption of individual node. The load distribution method balances the energy usage among the nodes and maximizes the network lifetime by avoiding over-utilized nodes at the time of selecting a routing path. In transmission power control approach, stronger transmission power increases the transmission range and reduces the hop count to the destination, while weaker transmission power makes the topology sparse, which may result in network partition and high end-to-end delay due to a larger hop count. Different energy-related metrics that have been used to determine energy efficient routing path: Energy consumed/packet, Time to network partition, inconsistency in node power levels, Cost/packet, and Maximum node cost. Some research proposals, which are based on transmission power control approach, are discussed in. Flow argumentation Routing (FAR) [8] which assumes a static network and finds the optimal routing path for a given source-destination pair that minimizes the sum of link costs along the path, Online Max-Min (OMM) [9] which achieves the same goal without knowing the data generation rate in advance. Power aware Localized Routing (PLR) [10] is a localized, fully distributed energy aware routing algorithm but it assumes that a source node has the location information of its neighbors and the destination and Minimum Energy Routing (MER) [11] addresses issues like obtaining accurate power information, associated overheads, maintenance of the minimum energy routes in the presence of mobility and implements the transmission power control mechanism in DSR and IEEE 802.11 MAC protocol. Few proposals to consider load distribution approach are given in [12, 13]. Localized Energy Aware Routing (LEAR) Protocol [12] is based on DSR but modifies the route discovery procedure for balanced energy consumption. In LEAR, a node determines whether to forward the route-request message or not depending on its residual battery power (Er). Conditional max-min battery capacity routing (CMMBCR) Protocol [13] uses the concept of a threshold to maximize the lifetime of each node and to use the battery fairly. Protocol not only provides a better way to discover Quality of Service and energy efficient route but it considers an efficient route maintenance scheme. Route maintenance has greatly enhanced the performance of the protocol in terms of network lifetime and packet delivery ratio [14]. In this proposed algorithm which maximizes the network lifetime by minimizing the power consumption during the source to destination route establishment. While discovering the path, destination waits for threshold time after receiving RREQ packets. During this time destination calculate link status ratio for every route from which it receives RREQ packet. Destination stores all possible route request for certain time, after the complete timer expire, selects path with the required link status ratio and reply to a path accordingly[15]. By selecting secured multiple paths with the removal of faulty links only and not the entire path, the reliability is enhanced and congestion gets reduced. Adaptive probe signals are used to find out the Byzantine Faults. Threshold is set based on the normal behavior of the network. When the loss rate exceeds the threshold, probing will start to find the adversaries. The paths from source to destination are then rated and the most trusted ones are selected for further communication [16]. Secure routing protocol for mobile ad hoc networks that achieves secrecy of data message and secures the routing operation. The security schemes aims at preventing attacks by malicious node that intentionally disrupt the route discovery process. The protocol also assures a source node generates a route discovery request is able to identify and authenticate the route reply from destination [17].To design a new secure routing protocol named ASRP, based on the SRP authentication protocol that we have employed to negotiate a secure connection using a user password, while eliminating the secure connection using a user password, while eliminating the results of simulation have demonstrated that ASRP offers good performance [18]. We have argued that previous solutions for securing routing MANETs have significant limitations, and presented SRDV as an instantiation of an approach based on end-to-end verification of path characteristics and the use of path diversity. SRDV addresses all of the security problems identified with prior approaches for secure routing in MANETs [19]. Use of multiple node-disjoint paths must consider the actual physical proximity of data transmissions on these paths. Four novel approaches were examined to improve data confidentiality and data availability: directional transmission, trans- mission power control, least-distance routing, and correlation factor control. It was demonstrated that the use of directional transmission and correlation factor control can greatly improve data availability by enhancing resilience to jamming and end- to-end fault tolerance, respectively [20]. We also analyze the security framework that was used for route discovery and argue. That compos-ability is an essential feature for ubiquitous applications [21]. Key management scheme for MANETs based on combining the threshold cryptography approach and the web of trust approach in one scheme. The proposed scheme exploits the routing process in executing the public key authentication. The proposed key management scheme provides redundancy since it is operable with and without the existence of the certificate authority and dynamically switches from a centralized scheme of trust to a distributed one [22]. Compare the performance of ad-hoc routing protocols in order to prove its correctness, efficiency, traffic load and end to end delay in dynamic intermediate nodes [23].The problem of providing QoS along with maximizing the network life and increasing the throughput by balancing the energy consumption [24]. During the problem of finding routes when nodes are moving in ad hoc network which results in consuming lot of system bandwidth and battery power. To overcome this, they have proposed new algorithm for maintaining routing table. It will respond to the changes in the network topology and adjusts the paths such that the lifetime of nodes can be maximized [25]. They proved that this protocol can not only effectively reduce energy consumption, thus prolong the network lifetime, but also significantly improve average end-to-end delay while maintaining a good packet delivery ratio [26]. Propose a proactive routing protocol which gives better performance and satisfies the basic power aware parameters like minimum energy consumption per packet, maximum network lifetime, and minimum variance in the node power levels [27]. However, AODV has limitation in security, thus it is susceptible to various attacks. One of the popular attacks in AODV is the Black Hole attack. There have been many works

done to secure AODV from this attack but there are still some issues that need to be addressed. In this paper proposed a novel method called ERDA (Enhance Route Discovery for AODV). ERDA will improve the security of the AODV during the route discovery process so that the adverse effect caused by the attack to the network performance is reduced [28]. The Relationship of this node with other nodes by introducing a perfect trust model in the network layer, we can establish secure route between source and destination without any intruders or malicious nodes [29]. In node based key management scheme is being used for securing nodes because nodes are the only medium to transmit packets to other mobile nodes. RREQ and RREP values are followed with node identification number for generating key [30]. Current key management schemes only consider the security of newly deployed nodes in wireless sensor networks, whereas the security of mobile nodes is ignored. In order to ensure data transfer secure in node mobility scenarios, we propose a composite security mechanism based on the elliptic curve digital signature algorithm to help nodes in the mobile scenarios to authenticate their identities and establish the pair wise keys [31]. A secure routing protocol named, ASRP, which based on reactive approach, means a node wants to send data to particular node it broadcast RDP to all its neighbor to finding the route, RDP contain address of destination, its own identity, timestamp t, nonce n, and it bind using its own private key to bind it [32]. Two-Fish is a 128 block cipher that accepts a variable-length key up to 256 key bits. The cipher is a 16-round Feistel network. No weak keys, Flexible design i.e. accept additional key lengths be implementable on a wide variety of platform and applications and be suitable for a stream cipher, hash function, simple design, both to facilitate ease of analysis and implementation. The result is highly flexible algorithm that can be implemented efficiently in a variety of cryptographic applications. Also Two-Fish Encryption Algorithm is public key on sender side and private key on receiver side with digital signature key so that data / packet is secure during transmission from sender to receiver [33,34].

3. SECURE POWER AWARE ROUTING

The proposed algorithm maximizes the network lifetime & minimizes the power consumption during the source to destination route establishment using a secure cryptographic method. This algorithm takes special care to transfer both real time and non real traffic by providing energy efficient and less congested path between a source and destination pair.

Functions Involved:

A) Explanation of Methodologies PAR

Current research works mainly focus on the selection of the path based on accumulated energy of all the nodes in that path. But while calculating this, one of the nodes in the path may have energy level below Power Aware Routing Protocol (PAR). This may result in death of the node after transmitting single or few packets. Need to the path be selected only if all of the nodes have energy level above or equal to some threshold value. Also as volume of data is known, energy level of each node after transmitting the data can be estimated. The path will be selected only if the entire node survives after transmitting the data. In the research paper [14] the criteria used for route selection is based on following parameters:

Step 1: Accumulated energy of path.

$$E_{ij} = \sum_{i=1}^{j-1} E_i \qquad (1)$$

Where E_{ij} is the residual energy of an intermediate node I, and E_i is the total energy of path form i to node j.

Step 2: Status of Battery Lifetime (B_S)

Step 3: Type of Data transfer:

a. Non Real Traffic (NRT)

b. Real Time (RT)

While selecting the route, destination waits for threshold time after request (RREQ) packet is arrived. During this time destination decides link status ratio by equation (1) for every arrived RREQ packet and stores all route request for certain amount of time.

A.1) Explanation of Design methodology PAR

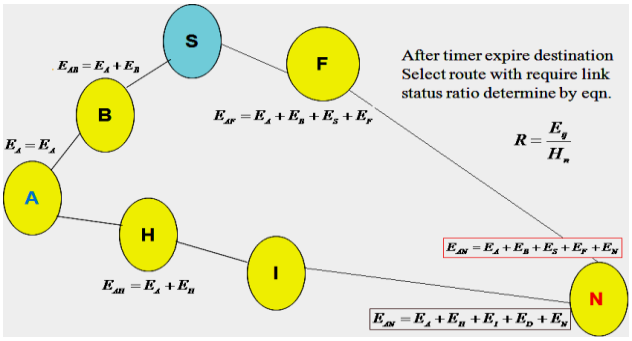

Figure 1: Design methodology of PAR

On expiry of the complete timer the destination node selects the route with required link status ratio and sends reply to select path. While selecting path on the basis of link status ratio of the route, which take summation of all nodes energy level, in that case there is possibility that one of the node may have energy level to low but due to accumulated energy calculation total energy seems to be of complete path at required level [14].

B) Explanation of Methodologies SPAR

Research work mainly focused on following points:

Step 1: Initially every node has some energy level, after transmitting packet it reduces its energy level.

Step 2: Along with the RREQ, source will send the total volume of data.

Step 3: Node will estimate its battery status, after transmitting the complete data.

Step 4: If found the energy level below the minimum require to survive, the path be discarded by blocking the RREQ.

Algorithm

If

$$E_{XM} > E_M$$

Then proceed

Else

Select alternate route.

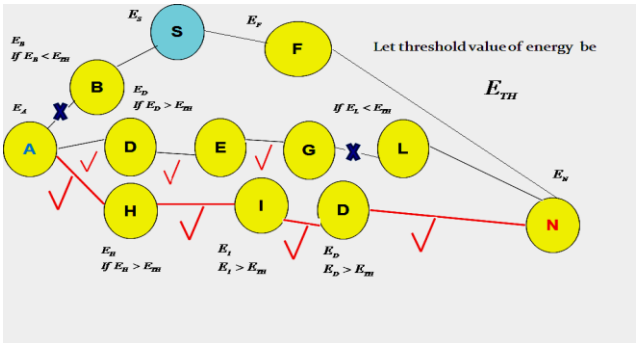

Figure 2: Methodology of SPAR

B.1) Explanation of Design methodology SPAR

Step 1: The estimation of battery status can be done from the details send by the node when it sends route request packet.

Step 2: In route request packet the header file has the following information.

Step 3: Source_id, Destination_id, Type of Data to be transfer, Total Battery Status, Total Traffic level and Node_id.

Step 4: Total traffic level is calculated from the packets buffered in the interface queue of the node.

Step 5: The battery status of node after transmitting known volume of data will be estimated.

Step 6: Let assume 1Joule is require to forward one packet.

Step7: While transmitting data from source, total packet to be transmitted will be send along with request node will calculate the remaining energy required.

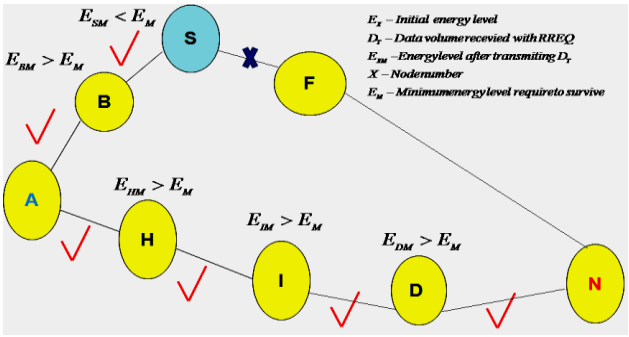

Figure 3: Design methodology of SPAR

Research works mainly focus on the selection of the path based on accumulated energy of all the nodes in that path. But while calculating this, one of the nodes in the path may have energy level below PAR. This may result in death of the node after transmitting single or few packets. Need to the path be selected only if all of the nodes have energy level above or equal to some threshold value. Also as volume of data is known, energy level of each node after transmitting the data can be estimated. The path will be selected only if the entire node survives after transmitting the data. While selecting path on the basis of link status ratio of the route , which take summation of all nodes energy level, in that case there is possibility that one of the node may have energy level to low but due to accumulated energy calculation total energy seems to be of complete path at required level. In such case the node will exhaust before completing the data transfer.

3.1 Parameters on Each Node

Each node has 3 variables: Node_ID, Battery Status (B_S)

and Traffic Level (T_L)

Battery status is further divided into 3 categories:

1) If (Battery Status < 20%)

Then Set B_S = 1.

2) If (20% δ Battery Status δ 60%)

Then Set B_S = 2.

3) If (Battery Status ε 60%)

Then Set B_S = 3.

3.2 Parameters to Concern during Route Search

At the time of route discovery, a route request (RREQ) packet broadcasted by the source. The header of the RREQ packet includes Source_id, Destination_id, T_O_L (type of data to be transfer), T_B_S (Total Battery Status), T_T_L (Total Traffic Level), and Node_IDs.

3.3 Calculation of Total Battery Status (T_B_S)

Initially T_B_S = 0 at source node. As RREQ packet propagates along the path, T_B_S is updated at each intermediate node i as follows:

If (B_Si == 3)

Then T_B_S = T_B_S + 3

Else-if (B_Si == 2)

Then T_B_S = T_B_S + 1

Else-if (B_Si == 1)

No updating is performed, and the node is not allowed to participate in the route discovery.

3.4 Calculation of Total Traffic level (T_T_L)

1) At a source node, Initially T_T_L = 0.

2) At the time of route discovery, add traffic status of each intermediate node to T_T_L.

Here traffic level (T_L) of a node is considered as number of packets buffered in the interface queue of the node.

3.5 Route Selection Criteria at Destination Side

The destination waits for a threshold time (Tth) after a RREQ packet arrives. During that time, the destination determines the link status ratio of the route for every arrived RREQ packet. Destination stores all possible route request for a certain amount of time. When the complete timer expires the

destination node selects the route with the required link status ratio and replies for a path accordingly with secured node. Here link status ratio of a path is calculated using equation (2).

$$R = \frac{E_{ij}}{H_n} \quad (2)$$

Where Eij is the total energy of a path from node i to node j as given In the equation (1)

Hn is number of intermediate hops along the path.

3.6 Energy Consumption Model

Energy consumption of a node after time t is calculated using equation (3):

$$Ec(t)=Nt*\alpha+Nr*ß \quad (3)$$

Where Ec(t) , energy consumed by a node after time t. Nt , no. of packets transmitted by the node after time t. Nr , no. of packets received by the node after time t.

α and ß are constant factors having a value between 0 and 1.

If E is the initial energy of a node, the remaining energy Er (t) of a node at time t, is calculated using equation (4):

$$Er(t)= E-Ec(t) \quad (4)$$

The following algorithm and flowchart describe this decision:

Algorithm: SPAR

If (T_O_L = = NRT)

Let N different values of R are received, where

Rε 1

If (N = = 0)

Send negative acknowledgement to the source that path cannot be established.

Else-if (N = = 1)

Acknowledge the source with this path.

Else-if (N > 1)

Select the path with min {T_T_L} and acknowledge the source with the selected path.

Else-if (T_O_L = = RT)

Let N different values of R are received, where

R ε 2

If (N = = 0)

Send negative acknowledgement informing that no such path is possible.

Else-if (N = = 1)

Acknowledge the source with this path.

Else-if (N > 1)

Select the path with Min {T_T_L} and acknowledge the source with the selected path.

Explanation of SPAR Flowchart:

Step 1: A signaling packet (RREQ/RREP) is received by node (A) from Node (H) looking for a path for destination (N).

Step 2: Node (A) extracts target (S/D) from signaling packet (If the signaling packet is a RREQ then the target is the source, if the signaling packet is a RREP, then the target is the Destination).

Step 3: Node (A) searches in routing table for another node (H) having a fresh route to the target.

Step 4: If the node (H) is not found or if the route is not fresh enough, an entry for the target node is added to the routing table of node (A).

Step 5: If the node (H) is found in the routing table, and has a route to the target the following should be verified:

a) How many times node (A) has used node (H) as a next hop (R1).

b) How many times node (A) has used node (N) as a next hop (R2).

c) Compare EXm and E_M.

d) Compare EXm > ET_H.

e) Compare R1 > R2.

f) Update Routing table.

g) Add node (A)'s cost to the signaling packet & forward it to the target node.

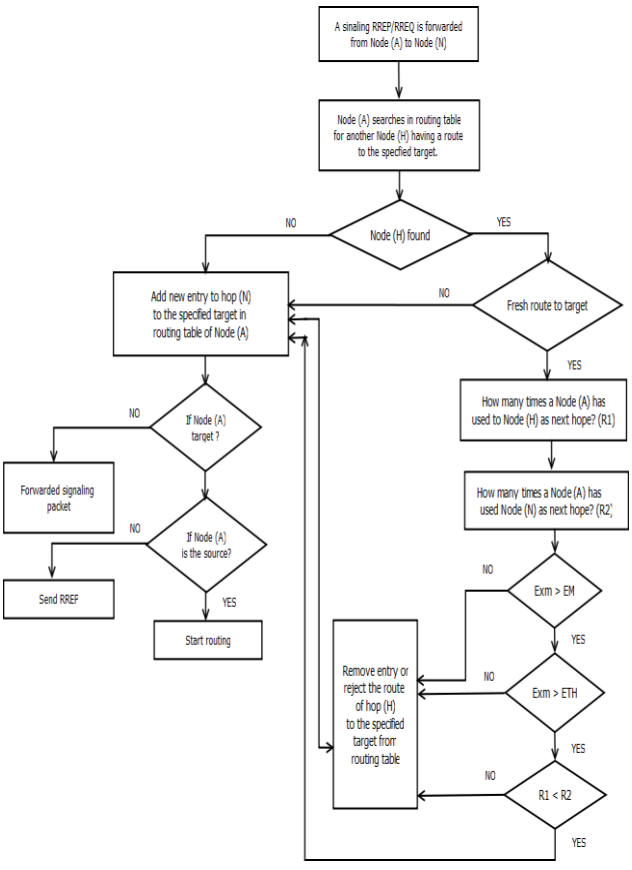

Figure 4: Flowchart for SPAR

4. TWOFISH ENCRYPTION ALGORITH

Security of networks depends on reliable key management system which generates and distributes symmetrical/ asymmetrical encryption/ decryption keys between communicating parties [35]. We designed Twofish cryptography algorithm in order to strengthen security in wireless communication environment. Design Twofish cryptography algorithm improved the existing MDS block with a MDS-M2 block that improved processor speed, and decreased complexity and power consumption [36]. The two main characteristics of a good encryption algorithm are: Security and Speed. Usually security algorithms have to be embedded in a variety of applications like e-banking, online shopping, mails etc. So they should be fast as well as secure in different environments. We do security v/s performance analysis of two algorithms Two-fish and AES [37]. We have shown that the actual distribution in one case was considerably less uniform than they had speculated, but that their other statistical con-jecture seems to be correct and also shown that these statistical properties do not apply to key sizes larger than 128 bits, and also argued that no cryptographic weaknesses in Two_sh result from these properties in the 128-bit key case [38]. To reconsider the di_culty of related-key and partial chosen-key attacks on reduced-round Two_sh [39]. Two-Fish uses a 16-round Feistel-like structure with additional whitening of the input and output. The only non-Feistel elements are the 1-bit rotates. The rotations can be moved into the *F* function to create a pure Feistel structure, but this requires an additional rotation of the words just before the output whitening step. The plaintext is split into four 32-bit words. In the input whitening step, these are XORed with four key words. This is followed by sixteen rounds. In each round, the two words on the left are used as input to the *g* functions - one of them is rotated by 8 bits first. The *g* function consists of four byte-wide key-dependent S-boxes, followed by a linear mixing step based on an MDS matrix. The results of the two *g* functions are combined using a Pseudo-Hadamard Transform (PHT), and two keywords are added. These two results are then XORed into the words on the right (one of which is rotated left by 1 bit first, the other is rotated right afterwards). The left and right halves are then swapped for the next round. After all the rounds, the swap of the last round is reversed, and the four words are XORed with four more key words to produce the cipher text the 16 bytes of plaintext *p*0…… *p*15 are first split into 4 words *P*0,..., *P*3 of 32 bits each using the little-endian convention.

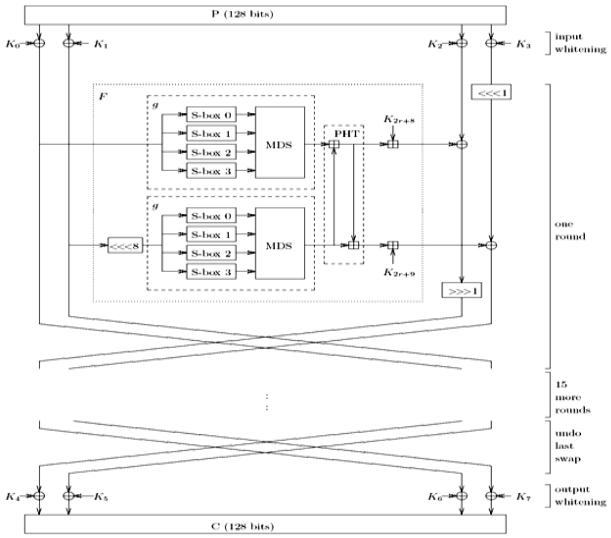

Figure 5: TwoFish [33]

Given two inputs, a and b, the 32-bit PHT is defined as:

$a' = a + b \bmod 2^{32}$

$b' = a + 2b \bmod 2^{32}$

Feistel Networks – the fundamental building block is the *F* function in equation (1):

i) A key-dependent mapping of an input string onto an output string.

ii) An *F* function is always non-linear and possibly non-surjective

$$F:\{0,1\}^{\frac{n}{2}} \times \{0,1\}^{N} \mapsto \{0,1\}^{\frac{n}{2}} \quad (1)$$

where *n* is the block size of the Feistel Network, and *F* is a function taking *n*/2 bits of the block and *N* bits of a key as input, and producing an output of length *n*/2 bits. In Two-Fish Encryption Algorithm we can use both public key and private key with digital signature. So that data / packet is secure during transmission from source to destination.

5. SIMULATION AND RESULT ANALYSIS

5.1 Simulation

The proposed scheme is simulated using network simulator NS-2[40] with latest version NS-2.34 and the performance is compared with well known on demand protocol AODV and the Power aware routing. Scenarios have been setup for 10, 30, 50 and 100 nodes in an area of 1000m*1000m. In the different scenarios from small network to large networks, value for packet delivery ratio has been observed by varying pause times from 0 to 500 and the speed has been changed form 1 meter per second to 25 meters per second. Mobile or Wireless network which have been used following values for different parameter:

Table 1: Simulation Parameter

Parameter	Value
Simulator	NS-2 Version 2.34
Simulation Time	100s
Number of Nodes	10,30,50,100
Routing Protocol	AODV , PAR
Traffic Model	CBR
Pause Time	0 to 500s
Mobility	1 m/s to 5 m/s
Terrain	1000m*1000m
Transmission Range	250m

Comparison Snapshot for AODV, PAR and SPAR:

In figure 1, figure 2 and figure3 shows snapshot for AODV, PAR and SPAR node 50. So here snapshot shows the comparison between AODV, PAR and SPAR. SPAR is better than AODV and PAR also security is more in the SPAR as compare to AODV and PAR Simulation is a fundamental tool in the development of MANET protocols, because the difficulty to deploy and debug them in real networks.

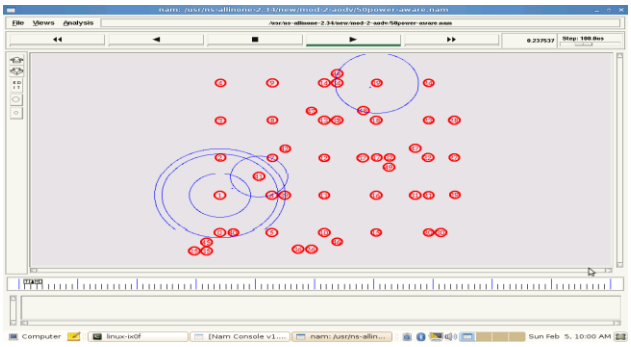

Figure 1: Snapshot for AODV node50

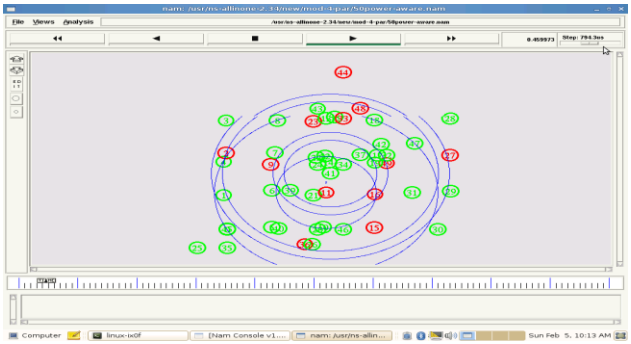

Figure 2: Snapshot for PAR node50

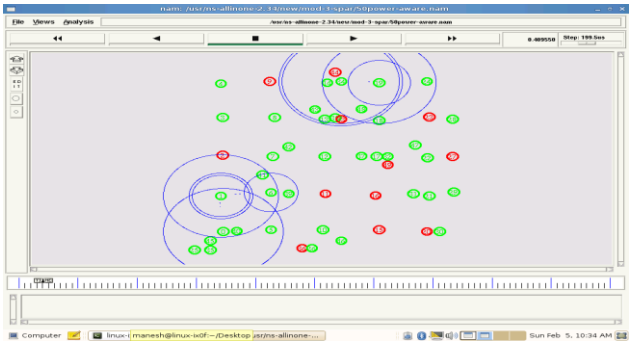

Figure 3: Snapshot for SPAR node50

The simulation eases the analyzing and the verification of the protocols, mainly in large-scale systems.

5.2 Results Analysis

Initially scenario has been setup for a 30 nodes network as shown in figure 1(a). As shown in figure 1(a) speed is constant and pause time is varied. In the beginning of the simulation, performance of AODV dips slightly; the reason can be delay in route reply messages due to high mobility of nodes and then once AODV Stabilizes it is delivering more packets. PAR scheme performs better as number of nodes increases. There is a slight delay in the start as it takes time to calculate the values for different parameters like power status, Traffic level, number of hops etc. Once initial calculations are done, PAR is able to deliver more than 97% packets all the time and at pause time greater than 250 it delivers approximately 99% packets. SPAR shows the similar results as compared to PAR. The dense medium changes some features of the protocols under study. As shown in figure 1(b) the performance of proposed algorithm 'SPAR' is best for 50 nodes proving the point that it was better to take care of factors like energy status and traffic level. Although initially packet fraction was very less when pause time was zero but later on as pause time increased performance of SPAR in much better as compare to AODV in terms of packet delivery. SPAR is delivering more number of packets for all speeds from 0 m/sec to 20 m/sec. The reason is again selection of a better path having less no. of hops, better energy status and minimum traffic level. SPAR uses IP level HELLO messaging to detect link breakages. If HELLO is not received within one second, the link is assumed to be broken. An active route timeout is after 50 seconds if unused. The reverse route lives less that is only 10 seconds. The route reply message should be received within one second after the request. If any of the nodes does not answer HELLO once, it is assumed that the link is broken. Route discovery is only tried three times. Request retransmits are done with three seconds intervals. Packets are held eight seconds while they are awaiting their routes to be discovered. Again, a node can send one route reply at each second. Energy status is attached with each HELLO packet; it is decremented by factor 0.025 each time a HELLO is echoed. Power status is attached with each HELLO packet; it is decremented by factor 0.025 each time a HELLO is echoed. Power status has been set at a scale of 7-10 at start for all nodes to be in active state. The entry is made in the route table at reply message stage. In case of proposed scheme route tables are updated at each Hello interval as in AODV with added entries for energy status and other factors. In figure 2(a) shows that the average End-to-End delay of AODV & PAR continuously increased in different number of nodes as compare to SPAR. In figure 2(b) shows that the

average End-to-End delay of AODV & PAR continuously increased in different number of nodes as compare to SPAR. The figure 3(a) shows that the performance of SPAR & PAR when the pause time is varies and the node speed is constant. Then see that throughput of SPAR is better than the throughput of AODV & PAR. In figure` 3(b) shows that throughput of SPAR is better than the throughput of AODV & PAR. Performance comparison of 'SPAR' with AODV and PAR in all above discussed scenarios is shown graphically in figure 1, figure 2, figure 3, figure 4 and figure 5. A special random scene has been considered in Figure 4, in this scenario all nodes are configured with different pause times and different speed and packet delivery ratio is observed by varying number of nodes as 10, 30, 50 and 100. Results show that the proposed scheme outperforms as the network grows and become larger and more dynamic. Even in case of a complete random scene the performance of SPAR is better than simple AODV and PAR as number of nodes increased in the network as shown in Figure 4. At last an experiment for a network of 30 nodes is performed for network lifetime. Network lifetime has been considered as the time in which a percentage of nodes are completely exhausted and the network is considered as a dead network. Simulation study is done for different speeds with constant pause time of 10 ms. Figure 5(a) and Figure 5(b) shows the comparison of network lifetime between simple AODV, PAR and SPAR with a speed of 2 m/s and 5 m/s respectively. It can be easily observed by Figure 5(a) that at a speed of 2 m/s, the network life time of SPAR is increased by 22.2% as compare to simple AODV therefore lifetime of proposed algorithm is increased with a good factor. While in Figure 5(b), it is clear that the network lifetime of SPAR is increased by 15.4% as compare to simple AODV. Although speed of 5 m/sec is fairly high in terms of energy consumption in a dynamic network but still SPAR is maintaining more network lifetime as compare to simple AODV.

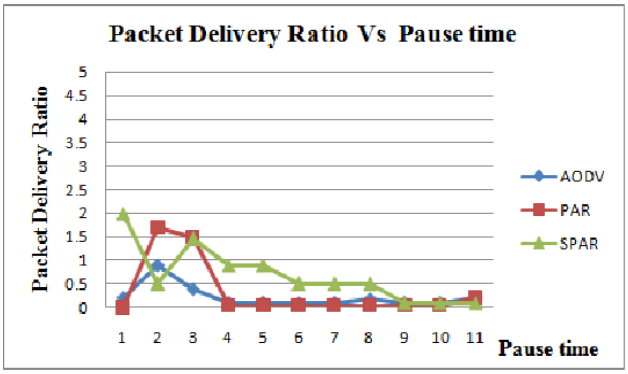

Figure 1(a): Packet Delivery Ratio for 30 nodes at different pause time

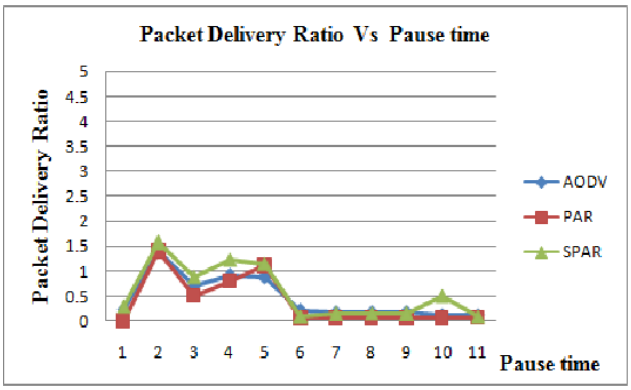

Figure 1(b): Packet Delivery Ratio for 50 nodes at different pause time

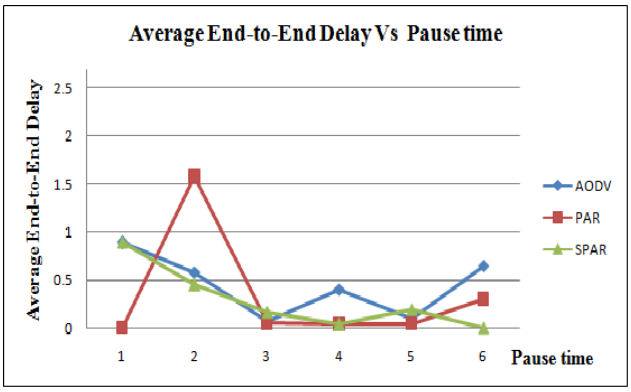

Figure 2(a): Average End-to-End Delay Vs Pause time for 30 nodes

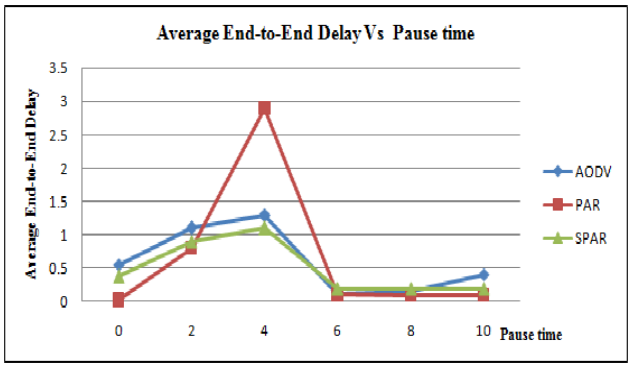

Figure 2(b): Average End-to-End Delay Vs Pause time for 50 nodes

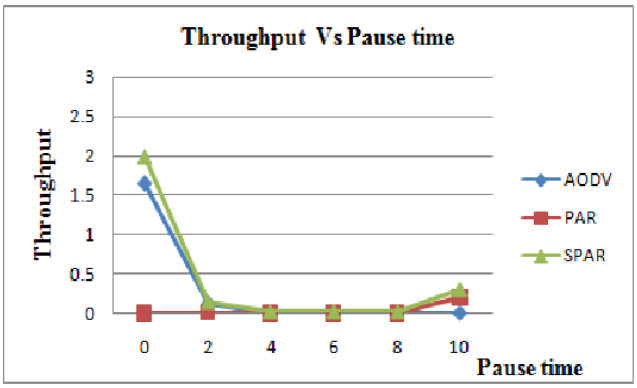

Figure 3(a): Throughput Vs Pause time for 30 nodes

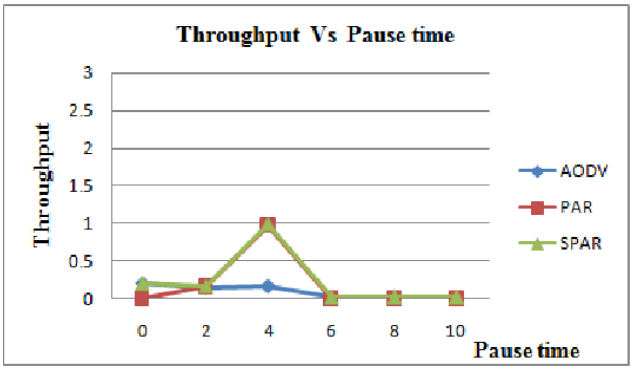

Figure 3(b): Throughput Vs Pause time for 50 nodes

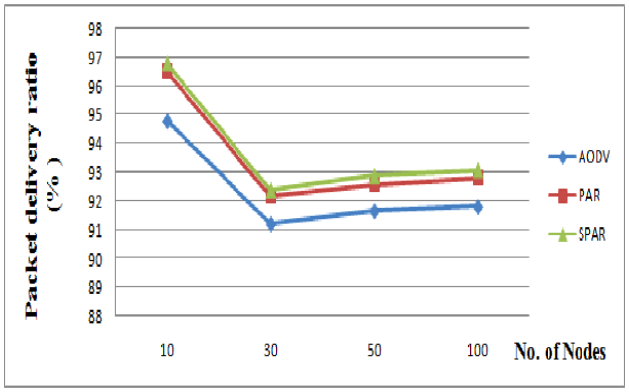

Figure 4: Packet Delivery Ratio for Random Scene

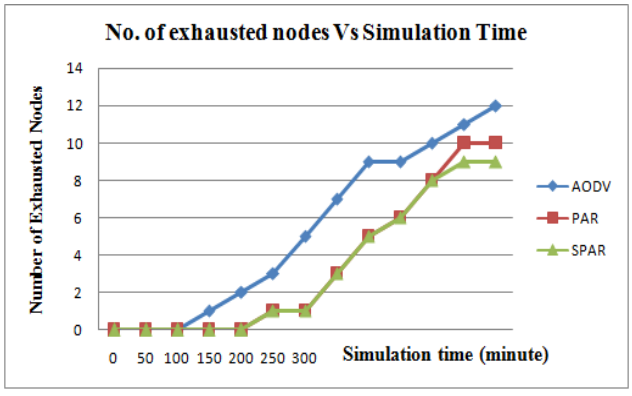

Figure 5(a): Simulation time vs. exhausted nodes with a speed 2 m/s

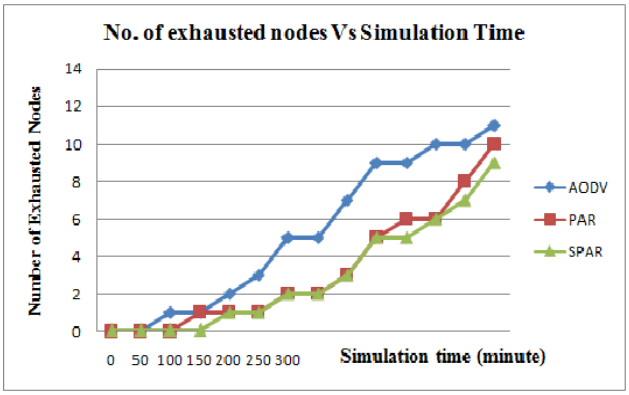

Figure 5(b): Simulation time vs. exhausted nodes with a speed 5 m/s

6. CONCLUSION AND FUTURE WORK

6.1 Conclusion

Energy efficiency is one of the main problems in a mobile ad hoc network, especially designing a routing protocol. The proposed work aims at discovering an efficient power aware routing scheme in MANETs and analyzing the derived algorithm with the help of NS-2. Simulation result shows that the proposed scheme SPAR is delivering more packets in different network scenarios as well as network life time of the SPAR, SPAR is better even in high mobility scenarios. Also protocol works especially well in terms of packet delivery and network lifetime. The process of checking the proposed scheme is on for more sparse mediums and real life scenarios and also for other metrics like Path optimality, Link layer overhead, total energy consumed etc. Although this scheme can somewhat enhance the latency of the data transfer but it results in a significant power saving and long lasting routes. This scheme is one of its types in ad hoc networks which can provide different routes for different type of data transfer and ultimately increases the network lifetime. In this protocol by using Two-Fish Encryption algorithm packets are secure while transmission from source to destination.

6.2 Future Work

In real time application of MANET, Service discovery is one of the issues needs attention. During earthquake all services are damaged at that time Ad Hoc network is work. If anyone needs service of medical facilities, from this Ad hoc network one node is having medical facility information is available and this information can be used. So that Service discovery is needed, and hence Service Discovery is the future work.

7. ACKNOWLEDGMENTS

It gives me proud privilege to complete this paper work. This is the only section where I have the opportunity to express my emotions and gratitude from the bottom of my heart. It is my great pleasure in expressing sincere and deep gratitude towards my guide **Prof. Praneet Saurabh, Asst. Prof.,** Department of Computer Science & Engineering, Technocrats Institute of Technology, Bhopal, for his valuable and firm suggestions, guidance and constant support throughout this work. I also offer my most sincere thanks to **Dr. Bhupendra Verma,** Director, Technocrats Institute of Technology, Bhopal.

8. REFERENCES

[1] Forman G., Zahorjan J.,"The Challenges of Mobile Computing," *IEEE Computer* 1994; 27(4):38-47.

[2] N. Sastry, U. Shankar, and D. Wagner, "Secure verification of location claims", I*n Proceedings of The 2nd ACM workshop on wireless security*, San Diego, CA, SA: ACM, pp.1-10, 2003.

[3] Ajina A, G. R .Sakthidharan, Kanchan M. Miskin, "Study of Energy Efficient Power Aware, Routing Algorithm and Applications", *Second International Conference on Machine Learning and Computing 2010*, vol., no., pp., 299-291, 2010.

[4] L. Abusalah, A. Khokhar, M. Guizani, "Trust Aware Routing in Mobile Ad Hoc Networks", *In Proceeding of Communication Society subject matter experts for publication in the IEEE GLOBECOM-2006*, 2006.

[5] Wenjing Lou, Wei Liu, Yuguang Fang, "A Simulation Study of Security Performance using Multipath Routing in Ad Hoc Networks", vol. no., pp. 2142- 2146, 2003.

[6] Perkins C., "Ad Hoc Networking" *Addison-Wesley*: 2001; 1-28.

[7] Chang J-H, Tassiulas L,"Energy Conserving Routing in Wireless Ad-hoc Networks," *Proc. IEEE International Conf. on Computer Communications (IEEE Infocom)* 2000; pp 22-31.

[8] Li Q, Aslam J, Rus D, "Online Power-aware Routing in Wireless Ad-hoc Networks," *Proceedings of Int'l Conf. on Mobile Computing and Networking (MobiCom'2001)*, 2001.

[9] Stojmenovic I, Lin X. "Power-Aware Localized Routing in Wireless Networks," *IEEE Trans. Parallel and Distributed Systems 2001*; 12(11):1122-1133.

[10] Doshi S, Brown TX, "Minimum Energy Routing Schemes for a Wireless Ad Hoc Network," *Proceedings of the Conference on Computer Communications (IEEE Infocom 2002)*, 2002.

[11] Woo K, Yu C et al., "Localized Routing Algorithm for Balanced Energy Consumption in Mobile Ad Hoc Networks,"*Proc. of Int'l Symp. on Modeling, Analysis and Simulation of Computer and Telecommunication Systems 2001*,117-124.

[12] Toh C-K,"Maximum Battery Life Routing to Support Ubiquitous Mobile Computing in Wireless Adhoc Networks,"*IEEE Communications 2001*.

[13] Vinay Rishiwal and Shekhar Verma,"QoS-Based Pure Adaptive Routing in MANETs", *IEEE International Conference on Emerging Trends in Engineering and Technology (IEEE ICETET 2008)*, 2008, 228-233.

[14] Vinay Rishiwal, Mano Yadav and Shekhar Verma, "Power Aware Routing to Support Real Time Traffic in Mobile Ad hoc Networks," *ICETET '08. First International Conference on Emerging Trends in Engineering and Technology*, vol., no., pp.223-227,16-18 July 2008JCS&T Vol. 9 No. 2, pp.101-109 Oct 2008.

[15] R. Sivakami, Dr. G. M. Kadhar Nawaz, "Secured Communication for MANETS in Military", *International Conference on Computer, Communication and Electrical Technology –ICCCET2011*, vol. no., pp., 146-151, 18th, 19th Mar. 2011.

[16] Rodríguez, Demóstenes Zegarra, Rosa, Renata Lopes, Lima, Pedro Hélio Medeiros de , "New Cache System-Based Power-Aware Algorithm in MANET," *Fifth International Conference on Digital Communication (ICDT)* , vol., no., pp.86-91, 13-19 June 2010.

[17] Keng Seng NG, Winston K. G.H. SEAH, "Routing Security and Data Confidentiality for Mobile Ad Hoc Networks", vol. pp., 1821-1825, IEEE-2003.

[18] Ahmed Nabet, Rida Khatoun, Lyes Khoukhi, Juliette Dromard and Dominique Gaïti, "Towards Secure Route Discovery Protocol in MANET," IEEE 2011,2011.

[19] Stephen Dabideen , Bradley R. Smith, J.J. Garcia-Luna-Aceves, "An End-to-End Solution for Secure and Survivable in MANETs", *7th International Workshop on the Design of Reliable Communication Networks*, vol. no., pp., 183-190,2009.

[20] Vladimir Berman and Biswanath Mukherjee, "Data Security in MANETs using Multipath Routing and Directional Transmission", *In Proceedings of IEEE Communications Society Subject matter experts for publication in the IEEE ICC 2006*,vol., no., pp. 2322-2328, 2006.

[21] Mike Burmester, and Breno de Medeiros, "On the Security of Route Discovery in MANETs",IEEE TRANSACTIONS ON MOBILE COMPUTING, vol. 8, no.9, pp., 1180-1188, Sept. 2009.

[22] Hisham Dahshan and James Irvine,"A Trust Based Threshold Cryptography Key Management for Mobile Ad hoc Network", 2009 -IEEE, 2009.

[23] Jahangir khan, Dr.syed Irfan Hyder, Dr.Syed Malek Fakar Duani Syed Mustafa, "Modeling and Simulation Of Dynamic Intermediate Nodes And Performance Analysis in MANETS Reactive Routing protocols," *International Journal of Grid and Distributed Computing* Vol. 4, pp.30-56, March 2011.

[24] P.K.Suri, M.K.Soni, Parul Tomar, "QOS Enable Power Aware Routing Protocol (QEPAR)," *International Journal of Engineering Science and Technology* Vol. 2(9), 2010, 4880-4885,2010.

[25] Seungjin Park, Seong-Moo Yoo, "Routing Table Maintenance in Mobile AD HOC Networks," *ICACT2010*ISBN 978-89-5519-146-2 issue Feb. 7-10, pp.1321-1325.

[26] Haojun Huang; Guangmin Hu; Fucai Yu; , "Delay-Sensitive and Power-Aware routing in wireless ad hoc networks," *International Conference on Communication Technology (ICCT)*, 2010 12th IEEE, vol., no., pp.496-499, 11-14 Nov. 2010.

[27] Murali P., Rakesh K., Hota C., Yla-Jaaski A., "Energy-aware routing in Mobile Ad-Hoc Networks," Wireless Days, 2008., WD '08.1st IFIP, vol., no., pp.1-5, 24-27 Nov. 2008.

[28] Kamarularifin Abd Jalil, Zaid Ahmad, Jamalul-Lail Ab Manan, "Securing Routing Table Update in AODV Routing Protocol", *2011 IEEE Conference on Open Systems (ICOS2011)*, September 25 - 28, 2011, Langkawi, Malaysia,2011.

[29] A. Menaka Pushpa, "Trust Based Secure Routing in AODV Routing Protocol", 2009 IEEE, 2009.

[30] S. Tapaswi , Virendra Singh Kushwah, "Securing Nodes in MANETs Using Node Based Key Management Scheme", *2010 International Conference on Advances in Computer Engineering,* vol., no., pp. 228-231, 2010.

[31] Xing Zhang, Jingsha He and Qian Wei,"Security Considerations on Node Mobility in Wireless Sensor Networks", *Fourth International Conference on Computer Sciences and Convergence Information Technology 2009,* vol., no., pp. 1143-1146, 2009.

[32] Tirthraj Rai, Ashish Jain, "Secure Routing in Mobile Ad hoc Network", International Journal of Computer Science & Communication, vol. 1, no.1, January-June 2010, pp. 125-127, 2010.

[33] Bruce Schneier, John Kelsey, Doug Whiting, David Wagner, Chris Hall, Niels Ferguson, "Twofish: A 128-Bit Block Cipher", In AES Round 1 Technical Evaluation CD-1: Documentation, NIST, 15th June 1998. See http: //www.nist.gov.aes.

[34] Doug Whiting, John Kelsey, Bruce Schneier, David Wagner, Niels Ferguson, Chris Hall, "Further Observations on the Key Schedule of Twofish", http://www.counterpane.com/twofish.html, Mar. 16, 1999.

[35] Kamal Kumar Chauhan, Shashikala Tapaswi, "A Secure Key Management System in Group Structured Mobile Ad hoc Networks", 2010 IEEE, vol., no., pp. 307-311, 2010.

[36] Pil-Joong Kang, Seon-Keun Lee, Hwan-Youg Kim, "Study on the Design of MDS-M2 Twofish Cryptographic Algorithm Adapted to Wireless Communication", vol., no., pp. 692-695, Feb, 20-22, 2006 ICACT 2006.

[37] Dr. S.A.M Rizvi , Dr. Syed Zeeshan Hussain, Neeta Wadhwa, "Performance Analysis of AES and TwoFish Encryption Schemes", *2011 International Conference on Communication Systems and Network Technologies,* vol., no., pp. 76-79,2011.

[38] Doug Whiting, John Kelsey, Bruce Schneier, David Wagner, Niels Ferguson, Chris Hall," Further Observations on the Key Schedule of Two_sh",vol.,no.,pp. 1-5, March 16, 1999.

[39] Niels Ferguson, John Kelsey, Bruce Schneier, Doug Whiting, "A Two_sh Retreat: Related-Key Attacks Against Reduced-Round Two_sh", vol., no., pp. 1-10, February 14, 2000.

[40] Eitan Altman and Tania Jimenez, Lecture Notes on,"NS Simulator for Beginners", December 03, 2003.