Journal of Theoretical and Applied Information Technology
10th October 2013. Vol. 56 No.1

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

ENSURING DATA CONFIDENTIALITY IN MANET BY COMBINING EMPHATIC CRYPTOGRAPHY TECHNIQUE WITH PSO

[1]SANDHYA P, [2]DR. JULIA PUNITHA MALAR DHAS
[1]Research Scholar, Noorul Islam university
[2]Professor, Noorul Islam university
[1]E-Mail: kiransandhya06@gmail.com

ABSTRACT

MANET is a dynamically varying network of wireless nodes that may move randomly independent of each other. Security, a serious crisis in MANET has innovative challenges such as data confidentiality and integrity. Malicious nodes or data hackers make packet dropping or interference in the routing messages in the network. To overcome these problems this paper proposes a secure optimized routing system with data confidentiality. Multipath route is optimized by selecting the best path using PSO (Particle Swarm Optimization) algorithm. Malicious nodes are identified by selecting the monitoring nodes derived from the network parameters: throughput bandwidth, and energy. Key management scheme with MD5 hash encryption is proposed to improve the secure data communication. The intent of MD5 algorithm is to generate the hash value for transmitting the data securely through the optimized route path. By simulation results, we show that the proficient of the proposed technique in terms of data confidentiality.

Keywords: *MANET, Data Confidentiality, Encryption, PSO (Particle Swarm Optimization), Malicious Node.*

1. INTRODUCTION

A group of mobile devices equipped with interfaces and networking competence is referred to as an Ad-hoc wireless network [1]. The merits of ad-hoc networks are quick deployment, strength, flexibility and essential support for mobility [2]. For a variety of applications, the simplicity of deployment and the lack of the requirement of any infrastructure make MANETs a striking preference [3]. Congestion became more demanding because of wireless links have considerably lower capability than wired links. This is due to the motivation that the mobile nodes communicate with each other through bandwidth constrained, variable capability, error-prone and self-doubting wireless channels [4].

Mobile nodes which are in the particular range within an ad-hoc network must work together to carry out some of the routine network services such as routing and security.

- The nature of nodes which are frequently embarrassed devices with restricted battery power and processing capabilities, so routing is an essential service that must be achieved by the ad-hoc network. Likewise, the nature of the area of consumption which is volatile and unbalanced makes the routing service as a challenging assignment.
- The second important service of MANETs is security, which is the most challenging charge to be passed out by the scientist society [5].

Routing is one of the centralized situations in wireless networks by attracting the consideration of researchers. The afford network connectivity routing use point-to-point multi-hop routing instead of a fixed network infrastructure [6]. A variety of routing protocols to have been projected for MANETs for unicast, multicast, multi-path and broadcast data transmission. The communication structures that are regularly determined to include: a path, a tree and a connected dominating set (CDS) [5]. In ad-hoc networks multipath routing, in which the first selective shortest paths are used for routing is better than the single path routing. This is achievable for the networks with a huge amount of nodes between any source destination pair of nodes [6]. Routing table overflow, routing table and cache poisoning are the routing attacks which can be performed by malicious node. In order to create the correct and proficient route between the pair of nodes routing protocols must be forceful against routing attack [7]. This brings up the requirement for protected routing protocols, where the Routing protocols must handle with such selfish and malicious activities [8].

There are so many algorithms are presented to solve this difficulty. There can be many routes from source to destination, but it is very hard to find any optimal path of minimum cost [9]. A novel idea of applying intelligence, which enables the nodes to take decisions is established and passed out the routing of the packets efficiently. The outcomes show that the routing approach along with PSO has achieved the optimal path with capable nodes. PSO is a technique of optimizing the routes, results iterative and trying to growth towards the concluding result [10].

By utilizing Particle Swarm Optimization for multipath routing, the best route will be selected based on the weight and priority of the nodes in the route. The minimum cost is calculated from source node to next node until it reaches the destination node. In PSO,

- Each particle is fascinated in the direction of finest position that it has personally found
- Each particle is fascinated in the direction of finest position that particle has ever found.

There is a need of security in any present network. However, the modern network environment without integrating with safety mechanisms has a number of security issues and lacks efficient security and integrity of data transferred over the network [11]. The recognition of attacks became a very complicated issue due to the need of centralized management in MANET. Mobile ad-hoc networks are highly forceful and large scale, and they cannot be easily monitored. Non malignant failures in MANETs are moderately common, e.g. communication destruction and packet dropping. As the outcome, malicious failures will be more complicated to detect. In a hostile environment, these unique characteristics of mobile ad-hoc networks increase challenges that security necessities must address, since security is a necessary component [12]. The directness of ad-hoc networks offers greater flexibility in terms of functionality, but it also provides an open path for any malicious node or hacker to get access to the network. Some of the least constraints should be met to pledge the secure operation of Ad-hoc network.

i) Authentication of a node is very essential so that the node can be trusted as a trusted node, and it is valid, and malicious. Eaves dropping nodes are denial access through the network.

ii) Data integrity is a main problem, to ensure the data communicated between nodes has not been distorted by any malicious node.

iii) Confidentiality is also required, to make sure that no intermediate node can access the data that is intended for the destination of that message [11].

Data confidentiality and data integrity are achieved by using encryption decryption algorithms for sending the files as confidential through the mobile ad-hoc network. The projected algorithm increases the data confidentiality by hash encryption of data [13]. Due to their selfishness attackers tries to hack the data or drop the data through network communication. Numerous counter measures such as strong authentication, encrypting and decrypting the messages using conventional cryptographic algorithms and redundant transmission can be used to attempt these attacks. Even though these traditional approaches be an important role in achieving confidentiality, integrity, authentication and non-repudiation, these are not sufficient for more sensitive applications and they can address only a subset of the threats [14].

Message integrity is one of the primary requirements in many of the today's network protocols. With the increment in network speed, higher processing speed is also essential for encryption, authentication and data integration. Presently various hash functions are being used for this reason, such as MD4, MD5 and SHA-1. Hash functions are very important cryptographic primitives and used in a number of fields of message integrity and signature confirmation. To achieve a fixed-size fingerprint or hash value of an arbitrary long message these methods are used. One way process and collision resistant are significant characteristics of hash functions. One way process indicates that the method to determine a hash value from a specified message is simple but it is computationally infeasible to produce any message that corresponds to a specified hash value [15].

MD5 is the one way hash function used to calculate the hash value for the message that the sender wants to send confidentially to the receiver. MD5 hash value is encrypted with the data and decryption is performed in the destination side. Asymmetric encryption algorithm is the public key encryption performs encryption with the MD5 hash value. The encrypted data with asymmetric key will be more data confidential. To solve the problems of key distribution the public key cryptography or asymmetric cryptographic technique is used. This method uses a private key and public key for encryption. The public key encrypts the data with equivalent private key for decryption. The private key kept secret and public key shared with others. If any node wants to send some information to other they should aware of the public key of that particular node and encrypts the information. After they receive the encrypted data, using their private key the information will be decrypted [16].

In this paper, PSO optimization for multipath routing technique is proposed for data confidentiality and integrity. Optimized route can obtain using this PSO algorithm by updating the position of each particle using the fitness function. From the optimized path the data transmission will take place after monitoring all the nodes for detecting the malicious node. An efficient cryptography technique called MD5 encryption is used to encrypt the packet based on message digest and private key. Then the corresponding packet can be decrypted only if the receiver knows the key.

Section 2 describes some of the related works based on data confidentiality in Mobile adhoc Networks. In section 3 we are concentrating on route optimization with Particle Swarm Optimization. Section 4 illustrates how to detect the malicious node by monitoring all the nodes. Section 5 demonstrates about the key management using MD5 hash encryption.

2 RELATED WORKS

Abhishek Toofani [9], have proposed a swarm intelligence technique called Particle Swarm Optimization to resolve routing difficulty, which gave the optimal path from the graph. Here discrete mathematics was used to predetermine particle in PSO, which broke search space in small search space and solved this discrete optimization. In the graph, there were a lot routes can exist from a source to a destination node. Among them discovering, the optimal path was a complex problem. It was an NP hard problem to find the route in a graph. T. R. Gopalakrishnan Nair and Kavitha Sooda [10] have proposed a grade based two levels based node assortment methods along with the Particle Swarm Optimization (PSO) methods. It assumed that the nodes were intellectual and there exist a knowledge base about the location in their local recollection. There were two levels for imminent the efficient route selection progression through grading. At the first level, grade based selection was applied and at the second level, the optimum path was explored using PSO. The simulation had been passed out on diverse topological structures, and it was observed that a graded network produced a considerable reduction to a number of iterations to enter at the optimal path selection.

Shiva Murthy G et al. [17] have proposed a protected node disjoint multi-path routing protocol for wireless sensor networks. Here, the data packets were transmitted in a protected way by using the digital signature crypto scheme. It was compared with an ad hoc on-demand multi-path distance vector routing protocol. It showed enhanced results in terms of packet delivery fraction, energy consumption, and end-to-end delay compared to the ad hoc on-demand multi-path distance vector routing. Subburaj.V and K.Chitra [18], have proposed an approach for node dynamism for implementing PSO based accessing system to obtain rid of attack exploitation for every node within the network. In Node's dynamism, all nodes were configured with PSO based fitness function, which will imitate on its gateway to circumvent various attacks like worm hole attack and web exploits, etc. To circumvent this type of attack, an exterior node (source of attack inspiration to misinform the transformation) when occupied in the Mobile attack has to be configured with node dynamism. This node dynamism also reflected on inside attack (a node knows the best route for an attack) struggle against it. The need for node dynamism also ensured node competent performance actions using rule based detection of individual nodes.

Aishwarya Sagar Anand Ukey and Meenu Chawla [19] has proposed a novel reputation based approach that deals with such routing misconduct and consisted of discovery and isolation of misbehaving nodes. Future approach can be incorporated on top of any source routing protocol and based on transferring acknowledgement packets and counting the amount of data packets of the active path. Routing protocol played a critical role for efficient communication between mobile nodes and operated on the basic statement that nodes are fully supportive. Because of this open arrangement and inadequate battery-based energy, some nodes (i.e. selfish or malicious) may not assist correctly.

Patrick Tague et al. [20] have proposed a framework for throughput optimization for multi-path uni-cast routing of wireless networks in the existence of probabilistic jamming. The framework introduced a numerical categorization into the maximum network flow crisis to balance for the decrease in network flow due to the loss of jammed packets. They mapped the difficulty of throughput optimization under probabilistic jamming to that of optimal investment portfolio selection, treating the network throughput as the revisit on financial investments and using a common portfolio selection framework from financial statistics. Based on the portfolio selection framework, they offered approaches to exploit expected throughput and to minimize throughput variance.

A. Jegatheesan and D. Manimegalaia [21] have proposed a new key management scheme that emphasized the safe and well-organized key updates by using a node Authenticated Symmetric Key Sharing approach. Furthermore, this scheme made use of a mixture of both symmetric and digital signature to guard other aspects of key management, such as data confidentiality, key distribution, etc. The proposed scheme exploited route reply messages in distributing symmetric keys between neighboring nodes in the reverse route from the destination node to the source node. The confidentiality of the distributed keys was sure by encrypting them with the recipient node’s public key. The digital signature was used to guarantee the legitimacy of the distributed keys.

3 MULTI-PATH ROUTING WITH OPTIMIZATION TECHNIQUE

Multipath routing is the routing methodology of using various alternative route paths through a network, which can give different benefits such as fault tolerance, increased bandwidth or enhanced security. Multipath routing is introduced for performing data transformation between source and destination using multiple route paths. Fig.1 shows the multipath for transfer a packet from source to destination. Route optimization is performed for this established multiple paths using PSO optimization.

PSO Algorithm

Kennedy and Eberhart developed an optimization algorithm called PSO, and this algorithm gets motivated by the shared behavior of bird flock. PSO algorithm observes input in a no of particles and in the case of networks; between two nodes multiple paths are established. Randomly selected particles (Sequence of nodes), serve as input to the PSO algorithm. Advantage of PSO algorithm is summarized as follows:

- not sensitive to scale the design variables
- easy implementation
- derivative free
- a small number of parameters required
- proficient global search technique.

Consider the network with the particular range consist of n no of particles.

Particle position, $P_n = (P_{n1,} P_{n2,....,} P_{np})$.

Particle velocity, $P_{vn} = (P_{vn1,} P_{vn2,}....,P_{vnd})$.

Particle best visited position, $P_n$best= $(P_{n1,} P_{n2,.......} P_{nd})$.

Global best position, $P_n$gbest = $(P_{g1,} P_{g2,........} P_{gd})$.

By using following equations update the position of the particle and its velocity

$$P_{vn}(t+1) = wP_{vn}(t) + C_{n1}\theta_1(P_n\text{best} - P_n) + C_{n2}\theta_2(P_n\text{best} - P_n)$$
(1)

$$P_n(t+1) = P_n(t) + P_{vn}(t+1)$$
(2)

Where, C_{n1} and C_{n2} - Positive constants

$P_n(t+1) = P_n(t) + P_{vn}(t+1)$- Two random variables $\in$ uniform distribution {0, 1}.

W - Weight of preceding velocity vector on the new vector.

The fitness value depends upon the bandwidth associated with the particles. The fitness value is calculated as below,

$$\text{Fitness}=\frac{B_{\text{Initial Link}}}{\sum_{i=0}^{t} \text{particle } B_t}$$
(3)

Where, $B_{InitialLink}$ is Initial bandwidth and B_t is Total bandwidth.

In this equation, limitation of velocity prevents the particle from moving too quickly from one region to another. This limited value is typically initialized as a function over the range of the crisis.

Consider a network. In a particular time period , a packet sent by one node typically traverses multiple routes before reaching its destination, and it may take a definite amount of time to traverse each path , making communication performance more efficient based on the network activities. Consider the role of optimization in controlling the routing of different paths through the Internet. Assuming the following (Fig.1) network type, and need to find the shortest path by optimizing the route. Each and every edge contains weight to calculate the minimum cost.

For example if the range of all P_{nj} is [-20, 20] then the maximum velocity is proportional to P_{nbest} 50 for each and every particle is updated based on the position in each iteration when a better position for the particle is obtained. The characteristic that drives PSO is social interaction. Particles within the network have the knowledge base and based on the knowledge obtain the best position. Individual within a neighborhood converse with one other when a new best position is found the P_{gbest} is updated.

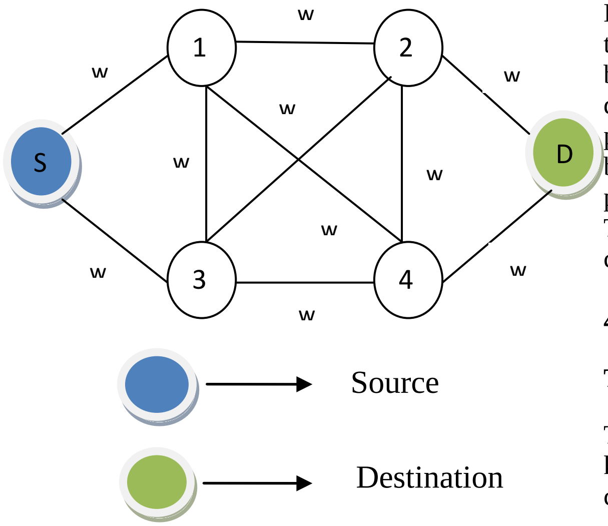

Fig.1. Multipath Network

The algorithm for the PSO is summarized as follows:

1. Initialize the swarm P_n, the positions of each particle are randomly initialized within the network.
2. Evaluate the performance F of each particle, using its current position P_n (t).
3. Compare the performance of each particle with the best performance

$$\text{Perfor}(P_n) < \text{Perfor}(P_n\text{best})$$
$$\text{Perfor}(P_n\text{best}) = \text{Perfor}(P_n)$$
$$P_n\text{best} = P_n$$

4. Compare the performance of each particle with the global best particle

$$\text{Perfor}(P_n) < \text{Perfor}(P_n\text{gbest})$$
$$\text{Perfor}(P_n\text{gbest}) = \text{Perfor}(P_n)$$
$$P_n\text{gbest} = P_n$$

5. Update the velocity of the particle using (1).
6. Change the position of the particle using (2).
7. Go to step 2, and repeat until convergence.

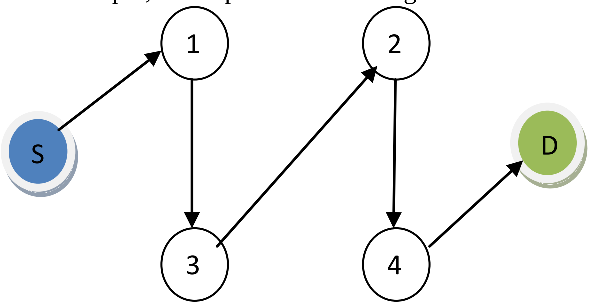

Fig. 2.Optimized Route Path

Based on the fitness function and weight assigned to the node the multiple paths get optimized. PSO based search algorithm with less iteration process decrease the chance of invalid loop or backward path. Each particle chooses its position explicitly based on the personal finest (pbest) from the particle's global finest (gbest) in the entire group. Thus choose the near shortest path in less computation time.

4 MALICIOUS NODE IDENTIFICATION

Throughput estimation

The packets get transmitted in a particular time is known as throughput. The network throughput is calculated using

$$TP \approx \frac{\text{Size of the window}}{\text{RTT}}$$

(4)

Round Trip Time is used to calculate the time to spend to transmit and delay to receive the packets, and it is calculated as,

$$\mathrm{RTT} = 2 * \mathrm{T}_{\mathrm{transmission}} + \frac{\mathrm{Distance}}{\mathrm{Propagation\ speed}} + \mathrm{Delay}_{\mathrm{processing}} (4a)$$

Where, $T_{transmission}$ is Time to transmit the packet, TP is throughput and RTT is Round Trip Time. Maximum propagation delay ≈ 0.5 µs

Energy estimation:

Total energy is calculated by using the division of following two parts

i.e. $E_{dis\,cov\,er-route}$ and r $E_{transmission-route}$.

$E_{dis\,cov\,er-route}$ is directly proportional to the number of packets.

Packet transmission taking place in a particular node consumes energy in four states. Those are as follows: (a) Transmit, (b) receive, (c) waiting state and (d) sleep. Energy in the active state is calculated by energy used for data transmission, and data receive processes. In sleep mode energy, status will be 0.Waiting state performs no operation.

$$\mathrm{E} \;\; = \mathrm{E}_{\mathrm{discover\text{-}route}} + \mathrm{E}_{\mathrm{transmission\text{-}route}}$$
(5)

$$\mathrm{E}_{\mathrm{discover\text{-}route}}\,\alpha \text{ no of packets}$$
(6)

$$\mathrm{E}_{\mathrm{transmission\text{-}route}} = \mathrm{E}_{\mathrm{tW}} + \mathrm{E}_{\mathrm{tA}} + \mathrm{E}_{\mathrm{tS}} + \mathrm{E}_{\mathrm{tT}}$$
(7)

$$\mathrm{E}_{\mathrm{tA}} = \mathrm{E}_{\mathrm{Active\text{-}Receive}} + \mathrm{E}_{\mathrm{Active\text{-}Transmit}}$$
(8)

$$\mathrm{E}_{\mathrm{tS}} \cong 0$$
(9)

Where, $E_{transmission-route}$ is the energy needed to transmit the packet to the next node. E_{tW} is the energy required for waiting state. E_{tA} is the energy required to transmit and receive packets. E_{tS} is sleep state in which no energy is needed. $E_{Active-Transmit}$ is the energy needed for packet transmission in a optimized path. $E_{Active-Receive}$ is the energy needed for receiving packet in a optimized path.

Bandwidth Estimation:

Compute the available bandwidth based on channel status within the network to find out the busy and idle periods of the network. By find out the channel usage of every single node and its neighbors, good approximation of the bandwidth usage can be obtained. The channel utilization ratio is defined by the fraction of channel busy period of time.

Calculate the channel utilization ratio $Util_{CH}$ for each time period T as

$$\mathrm{Util}_{\mathrm{CH}} = \frac{\mathrm{CH}_{\mathrm{busy}}}{\mathrm{T}}$$
(10)

Where, $Util_{CH}$ is channel utilization, CH_{busy} is period at channel busy and T is time.

Smoothing constant $\varphi \in [0,1]$, this defines to smooth the channel utilization, if the last channel utilization is $Util_{CH}$ (t-1). In current sampling window, the channel utilization ratio is $Util_{CH}$. Then, the current channel utilization ratio is calculated as

$$\mathrm{Util}_{\mathrm{CH}}(\mathrm{t}) = \varphi \mathrm{Util}_{\mathrm{CH}}(\mathrm{t}\,\text{-}1) + (1-\varphi)\mathrm{Util}_{\mathrm{CH}}$$
(11)

Channel utilization ratio $CH_{util}(t) \in$ 0 and 1. After calculating the channel utilization at time t, calculate the available bandwidth of a node at time t as

$$\mathrm{BW} = \mathrm{BW}_{\mathrm{CH}}(1 - \mathrm{Util}_{\mathrm{CH}}(\mathrm{t})) \qquad (12)$$

where, BW_{CH} is the raw channel bandwidth.

4.1 Monitoring Node

Monitoring nodes are represented to identify the status of all nodes. By using bandwidth and energy calculation select monitoring node, this is having best bandwidth and energy value. Monitoring node helps to identify the malicious activities taking place in the corresponding route path.

Let consider forward agent and backward agent. Initialize a forward agent at source node and forward through optimized route path for knowing about which is the best node by comparing bandwidth and energy of all nodes. Forward node passes through all nodes from source and collects the current status .Place the node's history such as bandwidth and energy in the forward agent record.

Table 1.Record of forward agent

FORWARD AGENT RECORD			
SOURCE ID	DESTINATION ID	AVAILABLE BANDWIDTH	ENERGY VALUE

When forward agent reaches the destination, destination node initializes the backward agent and traverse back to the source with the information that forward agent record contains. Table 1 and 2 represents the maintained records of forward and backward agents.

Table 2.Record of backward agent

BACKWARD AGENT RECORD			
SOURCE ID	DESTINATION ID	AVAILABLE BANDWIDTH	ENERGY VALUE

Source chooses the node with best available bandwidth and energy as a malicious node from the backward agent record. Fig 3 illustrates the selection of monitoring node N2 with maximum available bandwidth and residual energy is chosen as MoN.

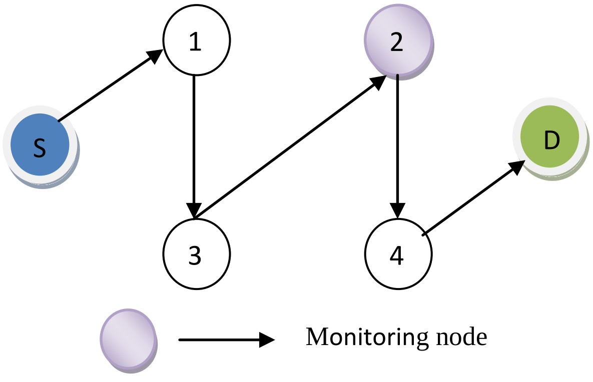

Fig 3.Selection of monitoring node

4.2 Malicious node

Monitoring node continuously monitors all the available nodes within the range and collects the status information to all nodes. At transmission of packet from source to destination, the subsequent condition should be checked. If the particular node satisfies the following condition, it can further transmit the packet through the corresponding path. Otherwise, the monitoring node will inform the node as malicious.

```
If  $(AB>AB_{th})$ && $(AE>AE_{th})$ && $(TP>TP_{th})$

Then

    Source $\xrightarrow{\text{Transmit packet}}$ Next node
Else

    Monitoring $\xrightarrow{\text{Warning message}}$ Source

EndIf
```

If the source node is ready to transmit the packet through the optimized path, it will check the above condition. First, the profile with the threshold values for bandwidth and energy the nodes must-have for the packet forwarding and the threshold value for optimal throughput. Compare the threshold values of bandwidth and energy with the available value. And also the throughput value should be higher than the profile value. If it is, then the corresponding node is capable to transmit the packet. When the source finds the node as malicious, it discards the further transmission as shown in Fig.4.

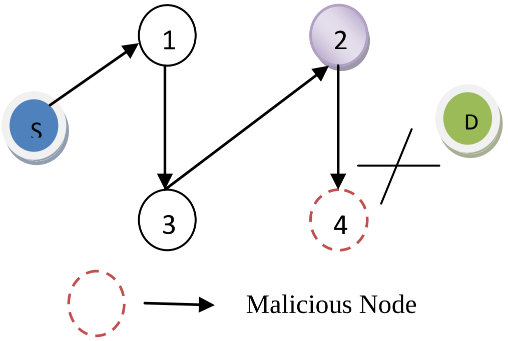

Fig.4. Detecting malicious nodes

The MoN (N2) detects N4 to be malicious node and sends the warning message to Source. Source while transmitting the data packets discards the path S – N1 - N3 - N2 - N4 – D and searches alternate route path for data forwarding.

5. KEY MANAGEMENT WITH CRYPTOGRAPHY

When the source receives the warning message, it will be alerted for hiding the packets from data hackers or intrusion. Here cryptography technique is introduced for preventing the data from unwanted sources. Cryptography technique includes secure encryption with MD5 hashing and decryption.

5.1 MD5 Algorithm for Secure Data Transfer

MD5 is the one way hash function used to find the hash value for the data to be transmitted. A hash function is a function that takes some message of any length as input and transforms it into a fixed length output called a hash value or a message digest. The MD5 algorithm is functioning as follows and depicts in Fig.5.

1. The data which we want to transmit is broken into 512 bit block division i.e. sixteen 32-bit little endian integers. The message length should be divisible by 512.The message is indicated by 64 bit representation.
2. Padding of message length:
A single 1 bit is added with message at the end.
3. Add zeros at the starting with this padding to bring the length into 512 bits totally.
4. The MD5 algorithm uses 4 state variables, each of which is a 32 bit integer (an unsigned long on most systems). The variables are initialized as follows:
A =67452301
B =EFCDAB89
C =98BADCFE
D =10325476.
5. Now on to the actual meat of the algorithm: the main part of the algorithm uses four functions
Those functions are as follows:
F(X, Y, Z) = (X & Y) | (~(X) & Z)
G(X,Y,Z) = (X & Z) | (Y & ~(Z))
H(X,Y,Z) = X ^ Y ^ Z
I(X,Y,Z) = Y ^ (X | ~(Z))
Where &, |, ^, and ~ are the bit-wise AND, OR, XOR, and NOT operators
6. These functions, using the state variables and the message as input, are used to transform the state variables from their initial state into what will become the message digest. For each 512 bits to the message, the rounds performed.
After this step, the message digest is stored in the state variables (A, B, C, and D). To get it into the hexadecimal form, output the hex values of each the state variables, least significant byte first. For example, if after the digest:
A = 0x01234567;
B = 0x89ABCDEF;
C = 0x1337D00D
D = 0xA5510101
Then the message digest would be:
67452301EFCDAB890DD03713010151A5.

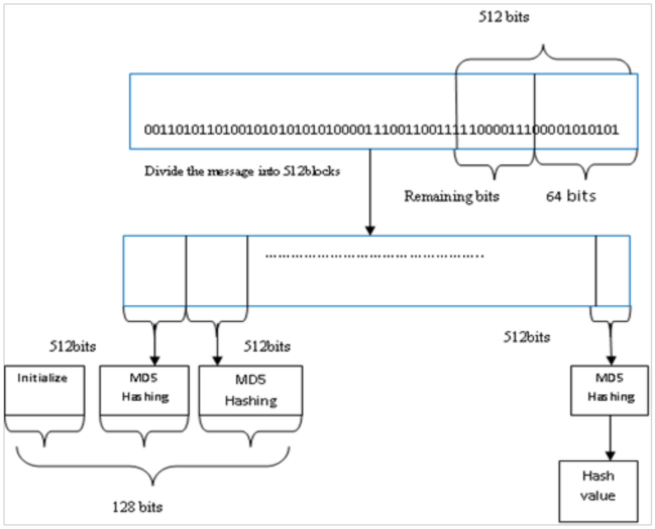

Fig.5. MD5 algorithm

5.2 Encryption

Source chooses a secret number (f), a large co-prime (u, v) and generates a common key (K_S) which is shown below.

$S_{prk} = p^{\alpha} \mod q$
(13)

Similarly, Destination chooses a secret number (g) and generates a common key (K_D) which is shown below.

$D_{prk} = p^{\beta} \mod q$
(14)

Both S and D possess common shared key which is generated as follows

$S_{puk} = p^{\alpha\beta} \mod q$
(15)

When source transmits the packet it calculates the hash value for the packet consisting data and encrypt the private key with this. Also encrypt the private key with the public key. Finally send this encrypted format to the destination. Pubic key get shared with both source and destination. Fig 6 presents the encryption procedure.

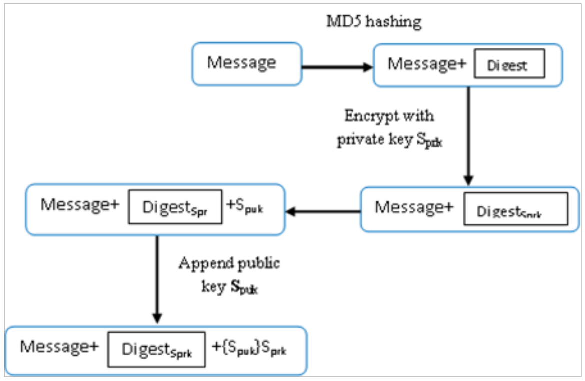

Fig.6. Encrypting data

5.3 Decryption

Each time node receives a data packet, it simply forwards this packet to the next node. After receiving the destination the packet will be decrypted if it has the private key. At destination node, from the public key extracts the sender's private key using the receiver's private key. Fig 7 presents the encryption procedure.

```
If Evaluated digest value == decrypted digest value
Then
            No alteration in the original data;
            Data confidential;
Else
            Data rejected as not an original data.
End If
```

This MD5 cryptography keeps data confidential from malicious activities in data transmission from source to destination.

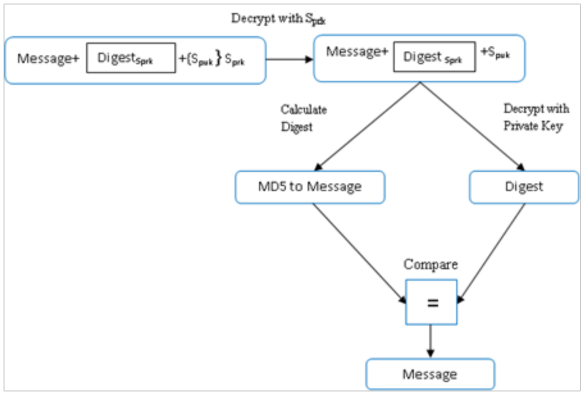

Fig 7.Decypting data

6 SIMULATION RESULTS

6.1 Simulation Parameters

We evaluate our Emphatic Cryptography technique with PSO for data confidentiality (ECTDC) through NS-2 [22]. We use a bounded region of 1000 x 1000 sqm, in which we place nodes using a uniform distribution. The number of nodes is 100. We assign the power levels of the nodes such that the transmissions range as 250 meters. In our simulation, the channel capacity of mobile hosts is set to the same value: 2 Mbps. We use the distributed coordination function (DCF) of IEEE 802.11 for wireless LANs as the MAC layer protocol. The simulated traffic is Constant Bit Rate (CBR).

6.2 Performance Metrics

We compare the performance of our proposed ECTDC approach with Normal Multipath technique. We evaluate mainly the performance according to the following metrics:

Average Packet Delivery Ratio: It is the ratio between the number of packets received successfully, and the total number of packets transmitted.

Average Energy Consumption: It is the average energy consumed by the nodes in receiving and sending the packets.

End-to-End-Delay: It is the amount of time taken by the packet to reach the destination.

Throughput: It is the number of packets received by the receiver during the communication process.

The simulation results are presented in the next section. Table.3 summarizes the simulation parameters used.

ISSN: 1992-8645 www.jatit.org E-ISSN: 1817-3195

6.3. Results & Analysis

A. Based on Attackers

In our first experiment, we analyze the metrics by varying the number of attackers as 1,2,3,4 and 5.

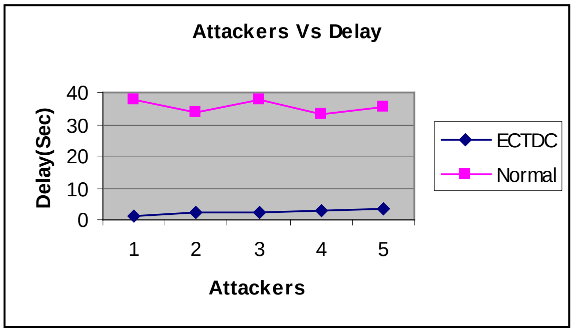

Fig.8. Attackers Vs Delay

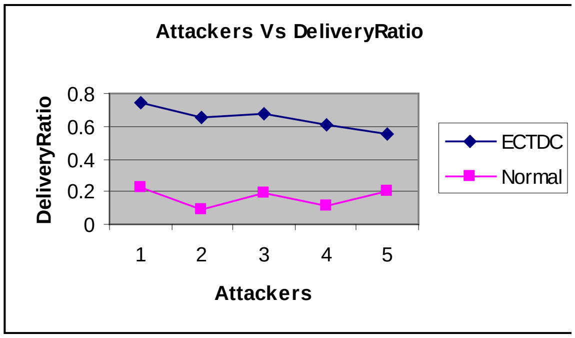

Fig.9. Attackers Vs Delivery Ratio

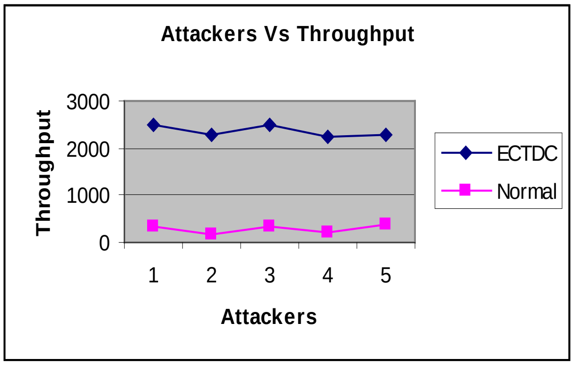

Fig 10. Attackers Vs Throughput

Table.3. Simulation parameters

No. of Nodes	100.
Area Size	1000 X 1000
Mac	802.11
Simulation Time	50 sec
Traffic Source	CBR
Packet Size	100,200,300,400 and 500.
Transmit Power	0.660 w
Receiving Power	0.395 w
Idle Power	0.035 w
Initial Energy	10.1 J
Transmission Rate	250m
Routing Protocol	ECTDC
Attackers	1,2,3,4 and 5.
Rate	100Kb.

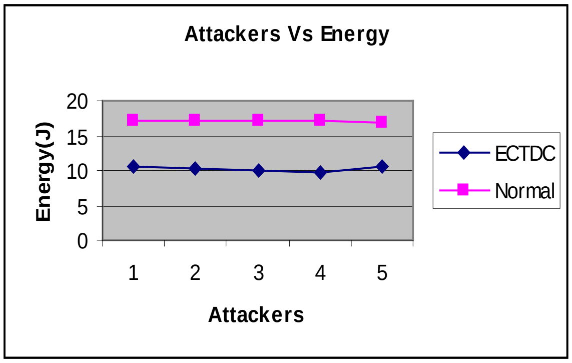

Fig.11. Attackers Vs Energy

From figure 8, we can see that the end-to-end delay of our proposed ECTDC is less than the existing normal scheme for various attackers' scenarios. From figure 9, we can see that the delivery ratio of our proposed ECTDC is higher than the existing normal scheme for various attackers' scenarios. From figure 10, we can see that the delivery ratio of our proposed ECTDC is higher than the existing normal scheme for various attackers' scenarios. From figure 11, we can see that the delivery ratio of our proposed ECTDC is higher than the existing normal scheme for various attackers' scenarios.

B. Based on Packet Size

In our second experiment, we analyze the metrics by varying the packet size as 100,200,300,400 and 500.

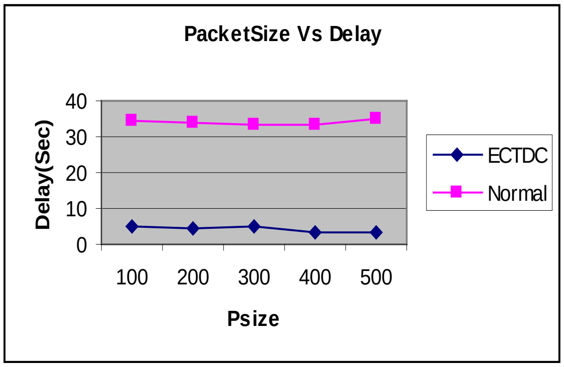

Fig.12. Packet Size Vs Delay

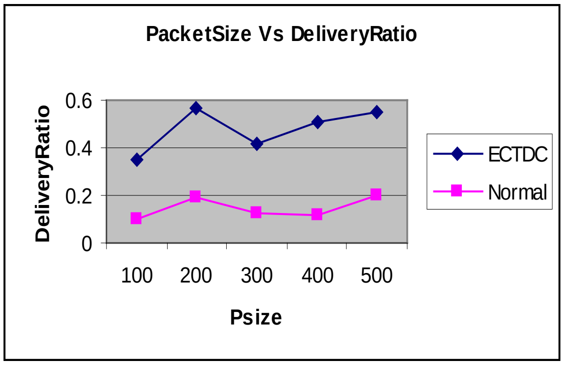

Fig.13. Packet Size Vs Delivery Ratio

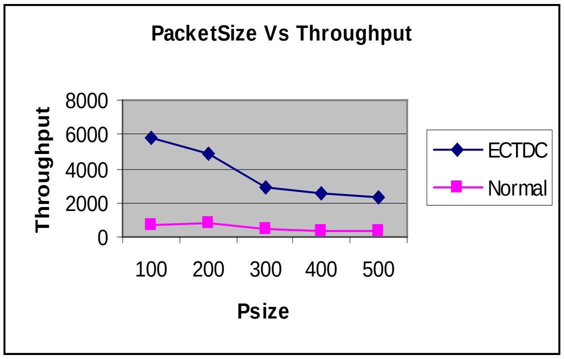

Fig.14. Packet Size Vs Throughput

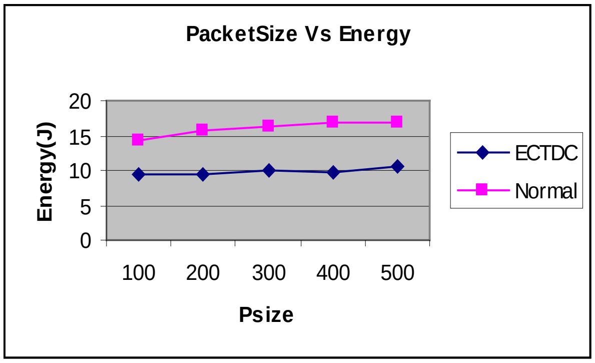

Fig.15. Packet Size Vs Energy

From figure 12, we can see that the end-to-end delay of our proposed ECTDC is less than the existing normal scheme for different packet sizes.

From figure 13, we can see that the delivery ratio of our proposed ECTDC is higher than the existing normal scheme for different packet sizes.

From figure 14, we can see that the throughput of our proposed ECTDC is higher than the existing normal scheme for different packet sizes. From figure 15, we can see that the energy consumption of our proposed ECTDC is less than the existing normal scheme for different packet sizes.

7. CONCLUSION

In this paper, we have proposed an emphatic technique for data confidentiality by using the optimal route for a secure data communication. To prevent data from unwanted sources or data hacker, multiple paths were optimized in order to select the shortest path according to the fitness function. From the optimized route, monitoring nodes are chosen from the calculation of bandwidth and energy. Monitoring node involved in the identification of malicious node and sent report to source node about the malicious activities. Source node forwarded the packet in the route which had found no malicious nodes in the corresponding path. For each packet which was transmitted through this optimized path were managed by using cryptography technique. Data were kept confidential due to this efficient method. Simulation results show that this proposed technique enhance data confidentiality more than the previous systems, mainly by improved data transmitting speed and by transferring data more confidential.

REFERENCES

[1] Sunil Taneja & Ashwani Kush,"Energy Efficient, Secure and Stable Routing Protocol for MANET," Global Journal of Computer Science and Technology Vol. 12 , pp.31-43, 2012.

[2] D. Jagadeesan and S.K. Srivatsa,"Multipath Routing Protocol for Effective Local Route Recovery in Mobile Ad hoc Network," Journal of Computer Science ,pp. 1143-1149, 2012.

[3] Chao Gui , Prasant Mohapatra,"SHORT: Self-Healing and Optimizing Routing Techniques for Mobile Ad Hoc Networks," In Proceedings of MobiHoc, pp. 279--290,2003.

[4] Soundararajan, S. and R.S. Bhuvaneswaran, "Adaptive Multi-Path Routing for Load Balancing in Mobile Ad Hoc Networks," Journal of Computer Science, Vol. 8, pp. 648-655 ,2012.

[5] Natarajan Meghanathan, "Graph Theory Algorithms for Mobile Ad Hoc Networks," Informatica ,Vol.36, pp.185-200,2012.

[6] Anju Gill and Chander Diwaker,"Comparative Analysis of Routing in MANET," International Journal of Advanced Research in Computer Science and Software Engineering,Vol. 2,2012.

[7] Preeti Sachan and Pabitra Mohan Khilar, "Securing AODV Routing Protocol in MANET Based on Cryptographic Authentication Mechanism," International Journal of Network Security & Its Applications (IJNSA), Vol.3, pp.229, 2011.

[8] Ahmed M. Abd El-Haleem and Ihab A. Ali ,"Tridnt: The Trust-Based Routing Protocol with Controlled Degree Of Node Selfishness for MANET," International Journal of Network Security & Its Applications (IJNSA), Vol.3, 2011.

[9] Abhishek Toofani, " Solving Routing Problem using Particle Swarm Optimization," International Journal of Computer Applications , pp. 16, Vol. 52, 2012.

[10] T. R. Gopalakrishnan Nair,Kavitha Sooda, "Particle Swarm Optimization for Realizing Intelligent Routing in Networks with Quality Grading," Wireless Communications, Networking and Mobile Computing (WiCOM), pp.1-4,2011.

[11] G. S. G. N. Anjaneyulu, V. Madhu Viswanatham and B. Venkateswarlu, "Secured and authenticated transmission of data using multipath routing in mobile AD-HOC networks," Advances in Applied Science Research, Vol. 2, pp.177-186, 2011.

[12] Hamza Aldabbas, Tariq Alwada'n, Helge Janicke, Ali Al-Bayatti, "Data Confidentiality in Mobile Ad hoc Networks," International Journal of Wireless & Mobile Networks (IJWMN) Vol. 4, 2012.

[13] Rohan Rayarikar,Ajinkya Bokil, "An Encryption Algorithm for End-to-End Secure Data Transmission in MANET," International Journal of Computer Applications ,Vol. 56, pp. 29-33, 2012.

[14] B. Shanthini,S. Swamynathan, "A Secured Authentication System for MANETs using Voice and Fingerprint Biometrics," European Journal of Scientific Research, Vol.59, pp. 533-546, 2011.

[15] Vandana Parihar, Dr. R.C.Jain, "Performance based Configuration and implementation of Hash Processor", International Journal of Advance Technology & Engineering Research (IJATER), Vol. 1, 2011.

[16] Amol Bhosle, Yogadhar Pandey ,"Applying Security to Data Using Symmetric Encryption in MANET," International Journal of Emerging Technology and Advanced Engineering,Vol. 3, 2013.

[17] Shiva Murthy G, Robert John D'Souza, and Golla Varaprasad ,"Digital Signature-Based Secure Node Disjoint Multipath Routing Protocol for Wireless Sensor Networks," IEEE SENSORS JOURNAL, Vol. 12,pp. 2941 - 2949 ,2012.

[18] Subburaj V, Chitra k, "Mobile Node Dynamism using Particle Swarm Optimization to fight against Vulnerability Exploitations," International Journal of Computer Applications, Vol. 41, 2012.

[19] Aishwarya Sagar Anand Ukey, Meenu Chawla,"Detection of Packet Dropping Attack Using Improved Acknowledgement Based Scheme in MANET," IJCSI International Journal of Computer Science Issues, Vol. 7, 2010.

[20] Patrick Tague, Sidharth Nabar, James A. Ritcey, David Slater, and Radha Poovendran, "Throughput Optimization for Multipath Unicast Routing Under Probabilistic Jamming,"Personal,

Indoor and Mobile Radio Communications, 2008. PIMRC 2008. IEEE 19th International Symposium on, pp. 1-5, 2008.

[21] A. Jegatheesan and D. Manimegalai,"Symmetric Key Management for Mobile Ad hoc Networks using Novel Secure and Authenticated Key Distribution Protocol," European Journal of Scientific Research, Vol. 88 , pp.334-345, 2012.

[22] Network Simulator: http:///www.isi.edu/ns/nam