B-LoDiS Routing for Intermittently Connected MANET with Agent AES Approach

S. Ramesh[1], R. Indira[2]

[1] *Faculty/CSE, Regional Centre of Anna University, Madurai, INDIA*
[2]*Assistant Professor/CSE, Adhiyamaan College of Engineering, Hosur, INDIA*

Abstract- **The Wireless and the Mobile Networks appear to provide a wide range of applications. Following these, the Mobile Ad hoc Networks (MANET) aid in wide development of many applications. The achievement of the real world applications are attained through effective routing. The Intermittently Connected Mobile Ad hoc Network (ICMANET) is a sparse network where a full connectivity is never possible. ICMANET is a disconnected MANET and is also a Delay Tolerant Network (DTN) that sustains for higher delays. The routing in a disseminated network is a difficult task. A new routing scheme called Bee Routing Protocol in amalgamation with storage scheme LoDiS is been proposed with a motto of achieving optimal result in delivering the data packet towards the destined node. The routing is termed is B-LoDiS. Though routing is adapted, the technique of secure routing remains an issue. In regard to this context, in this paper, a mechanism of secure routing is explored by means of Agent Technology. Agent is set at each node and it acts as a middle man in detecting the malicious node in the network. To enhance the mode of secure communication in larger scale, a Cryptographic algorithm Advanced Encryption Standard (AES) is adapted. AES with Agent Technology possibly increases the efficiency of routing excluding intruders. The degree of security is proved by testing with malicious nodes in the network considering their mobility and maximum number of nodes in the network. The main objective is to ensure secure routing with enhanced performance.**

Index Terms— AES, Agent, BCO, B-LoDiS, Delay Tolerant, ICMANET Network, MANET.

I. Introduction

A Mobile Ad hoc Network (MANET) is a collection of autonomous mobile nodes connected by means of Wireless medium. The nodes in this network are seemed to be organized in a decentralized manner. The nodes communicate with each other through links connecting the intermediate nodes available between the source and destination nodes. Connection through intermediate nodes is mainly due to the limitation of data transmission existing in the wireless environment.

In general, routing in a temporary network topology is a difficult task. Many traditional routing protocols viz., Distance Vector, Link State routing (LSR), Ad hoc Ondemand Distance Vector (AODV), Distance Source Routing (DSR), Opportunistic Adaptive Routing, Open Shortest Path First (OSPF) routing etc are been proposed since last decades. These routing protocols ensure effective data communication. MANET araise from mobile network and it leads to a disconnected network called the Intermittently Connected Mobile Ad hoc Network (ICMANET).

ICMANET is a typical Delay Tolerant Network (DTN), a network that incurs larger delays. It is designed to operate effectively over extreme distances such as those encountered in sparse communication or an interplanetary scale. The sparse or dense network of intermittent network is mainly due to high mobility of the nodes. The nodes stir within fractions of time and hence their topology changes in a dynamic way. Typical examples of intermittent network are wild life tracking, habitat monitoring sensor network, military network, nomadic community network and vehicular network etc. Due to typical distorted nature of the network, routing becomes an onerous task.

Many routing protocols are been proposed for communication in ICMANET since past years. The routing techniques are namely Flooding, Epidemic, Direction Based Routing, Adaptive Routing, Utility based Routing, Probabilistic Routing, Copy Case Routing, Spray and Wait Routing, LAROD-LoDiS etc. All the above mentioned routing protocols adopt a proficient mode for data communication. But the means of secure communication is not in effect.

The secure communication in MANET adhere enormous technical challenges due to unique characteristics of MANET. In addition to that it opens for eaves dropping due to intermediate communication and also holds many security threats. Hence security in MANET is adopted using Intrusion Detection System (IDS) or by creating a Trust [25] based environment. The IDS shows extended varieties like Behavior based IDS [26], Knowledge based IDS [26], Distributed IDS [27], Real –Time IDS [27], Multi – Layer Integrated Anomaly Detection System [28], Clustering Approach [29], Mobile Based Detection System [30], Co-operative Approach [31] etc. These known systems enhance the secure communication in MANET.

The security protocols designed for MANET are not suited for ICMANET which is mainly due to the disconnected nature of the network. Since the trust based system, IDS all require a central server to ensure authentication. The impossibility of setting central server in ICMANET does not adopt these techniques. Hence a new mode of security protocol is to be designed that does not demand for a central system.

In this paper, we propose a novel security protocol for ICMANET. Agent is set at each node, which has few authentication terminologies, any node that passes the terminologies are assured to be the trusted node. The data is encrypted preceding the transmission. The Encryption-Decryption is made through the Advanced Encryption Standard (AES) algorithm. Thus without setting a central server, a secure communication is achieved in ICMANET.

This paper is organized as the following sections. Section II describes the Related Work for routing in ICMANET. The protocol terminologies are discussed in Section III. Section IV describes the mechanism of secure routing. The performance evaluation is portrayed in Section V.

II. Related Work

The Intermittently connected network is a new form of emerging network where routing data packets is seemed to be monotonous task. Many research works have proved the possibility of routing in ICMN. This section provides an overview of routing techniques applicable in the intermittent network. The routing techniques vary at a larger rate from the traditional routing protocols. The routing protocols of ICMN should include the main feature of tolerating higher delays as the connectivity is transient in nature. Some of the intermittent routing protocols are described as follows.

The traditional routing scheme that forms a basis for the routing schemes in ICMANET is the Flooding based routing. In this, one node sends packet to all other nodes in the network. Each node acts as both a transmitter and a receiver. Each node tries to forward every message to every one of its neighbors [15]. The result in every message eventually is delivered to all reachable parts of the network.

The Epidemic routing oeuvres on the basis of the traditional flooding based routing protocol, which states that periodic pair – wise connectivity is necessitate for message delivery [13]. The protocol banks on immediate dissemination of messages across the network. Routing occurs based on the node mobility of carriers that are within distinctive position of the network.

The Beaconless routing protocol [12] is grounded on the hypothesis where there never exists an intervallic diffusion of beacons into the network. Routing primarily makes a choice of forwarding node in a dispersed modus amidst its neighbors, without any form of erudition about their location or prevalence.

The Context Aware Routing (CAR) [11] algorithm paves the forethought of asynchronous communication in ICMANET. The algorithm endows a basement of organizing the messages in the network. It addresses that the nodes are able to exploit the context information to make local decisions which imparts the good delivery ratios and latencies with less overhead. CAR is pain staked as a general framework to predict and evaluate context information for superior delivery of messages.

The Brownian Gossip [10] is an amalgamation of gossip and the random node mobility which provides a scalable geographical routing. In this routing, each node forwards the query related to other nodes information with certain values of probability. Gossiping is a resourceful approach for information dissemination and is done with a probability viz., Pgossip. The probability value makes certain that the query can reach the secondary nodes in the network with highest probability.

The Mobility Profile Based routing [9] addresses, a hub – level routing method and two versions of user – level routing methods [14].The routing involves a SOLAR–HUB (Sociological Orbit aware Location Approximation and Routing) which manipulates the user profiles that aids in hub – level routing.

The Direction Based Geographic Routing (DIG) [8] algorithm is grounded on geographic location of packets that are routed in an average approximate ideal path towards destination. The algorithm postulates that when two nodes encounter each other, the nodes exchange the knowledge of their current location, moving direction and the packets. The packets are forwarded to nodes whose distance and moving direction are closest to destination.

The Single Copy Case routing [7], from its nomenclature it postulates that only a single copy of message packet is carried to destination. The routing scheme includes direct transmission, randomized routing, utility based routing, seek and focus and Oracle based routing.

The Multiple Copy Case [6] scheme deals with the mechanism of spraying a few copies of message and then routing each copy in isolated manner to the destination. The algorithm that holds multiple copy case routing are Spray and Wait and Spray and Focus.

The Semi Probabilistic Routing (SPR) [5] algorithm considers that the network is partitioned into tiny portions that have a stable topology. The protocol upholds the information about host mobility and connectivity changes for more accurate message forwarding.

The Contention Based Routing postulates that the efficiency of routing can be achieved only by taking into account the contention and dead end [4].The Spray Select and Focus provides a better performance considering the contention and dead ends.

The Spray and Hop [3] is a routing protocol that holds two phases namely, Spray phase that sprays few copies of message into the network. Hop phase which occurs after the spraying phase, a node that was not able to find the destination, switches to the hop phase.

The Spray and Wait [2] is a scheme that sprays into the network a fewer number of message copies and waits until one of these nodes that holds the copies reaches the destination. It is simple to implement and can be optimized to achieve the depicted performance.

The LAROD-LoDiS [1] routing is a geographical routing that uses a Beaconless routing protocol and a Store Forward Carry technique. It also uses a database to communicate among them to achieve routing. It is done by Gossiping protocol. It provides constant overhead and higher delivery ratio.

These routing techniques do not pave a way for secure communication. To enhance the mode of secure communication, in this paper we proposed the agent technology for providing authentication and to ensure additional security for data AES algorithm is used with B-R, routing protocol based on Bee Colony Optimization (BCO). The security in network plays an imperative role in preventing threats or data theft by the intruders. The privation for security is essential in network communication.

III. Terminologies Of Protocol

The Section III depicts the various terminologies that were adapted for secure routing in ICMANET. The terminologies mentioned include B-LoDiS, Agent working, infrastructure and its principle and general description of AES algorithm.

A. B-LoDiS Routing Protocol

The B-LODIS is a routing protocol which operates based on BCO, an optimization technique. In this section, the general procedure of Bee working is depicted in sequence to this is the introductory.

BCO [35] is an optimization technique under the swarm intelligence, a part of Artificial Intelligence which is based on the actions of individuals in various decentralized systems. The decentralized system is composed of individual systems that are capable to communicate, cooperate, collaborate and exchange information among them. BCO [35] is a “bottom-up” [36] approach. Artificial bees are created in BCO that acts as artificial agents inspired by the general behavior of natural bees aiding in the solution for optimization problems.

The natural bees operate in such a way described as follows. The bees perform a dancing ceremony called the waggle dance. The waggle dance [37] acts as the communication medium among bees notifying about the quantity of food collected and the closeness of the path. When a bee finds a source of food, on its return to the hive, the bees dance in a figure eight pattern [36]-[37]. The waggle dance is repeated for a few numbers of times. The dance informs the details about the distance and the angle towards the food source. Direction and distance are estimated by the angle of distance relative to sun position and the length of the straight waggle run respectively. With the general bee movement and behavior the BCO algorithm is formulated by experts as follows.

BCO [38] is inspired by the natural behavior of bees and is a population-based algorithm. The basic idea behind BCO is to create a group of artificial bees. The artificial bees represent agents, each generating a new solution. The process is to generate an optimal solution. The BCO [38]-[40] algorithm consists of two phases namely the forward and backward phases respectively. The forward phase is a search phase during which artificial bees undergoes a predefined number of moves, constructing the solution and hence yielding a new solution. The new solution obtained is the partial solution. The artificial bees then start the backward phase, where they share information about their solution with each other. The information sharing is estimated by the objective value function.

The pseudocode for BCO [42] is portrayed in Fig. 1 as follows. The algorithm involves three steps namely performing the dance, estimating the path with the aid of dance and observing dance. The sequences of steps are repeated to find an optimal solution with all the partial solutions available from each artificial bee.

```
Procedure BCO()
Initialize_Population()
   While stop criteria are not fulfilled do
      While all bees have not built a complete path do
         Observe_Dance()
         Forage_ByTransRule()
         Perform_Waggle_Dance()
      End While
   End While
```

Fig. 2 Pseudocode for BCO

B. AGENT TECHNOLOGY

The Agent is a program module that functions incessantly in a meticulous environ [19]. It is proficient in carrying out activities in a supple and intellectual comportment, that is responsive to changes in the surrounding environ. The agent is not a complete program but is an interface [16] responsible for performing the pre assigned chores. Agent is autonomous which takes actions grounded on its innate knowledge and its precedent experiences [18].

On setting agent at each node, security [20] is achieved by incorporating certain agent parameters at each node. The agent parameters [32] are described as follows:

I. Node ID – A unique identifier for each node in the network.

II. Passcode – A common password for the nodes in the network.

III. Mobility Model – The mobility model of the network topology.

IV. Origin of Placement – The initial placement of each node in the network.

V. Grid Card – An n x n matrix in which each grid contains a particular data in it. Each node contains a unique grid.

VI. Pattern Formation – The network is associated with certain geometric silhouettes and using these, each node encompasses a unique pattern.

These agent parameters settle on the security issue coupled in the ICMANET.

Agent is set in each node and it includes three components [17] [32] namely:

i. Data Aggregator.
ii. Node Analyzer.
iii. Data Broadcaster.

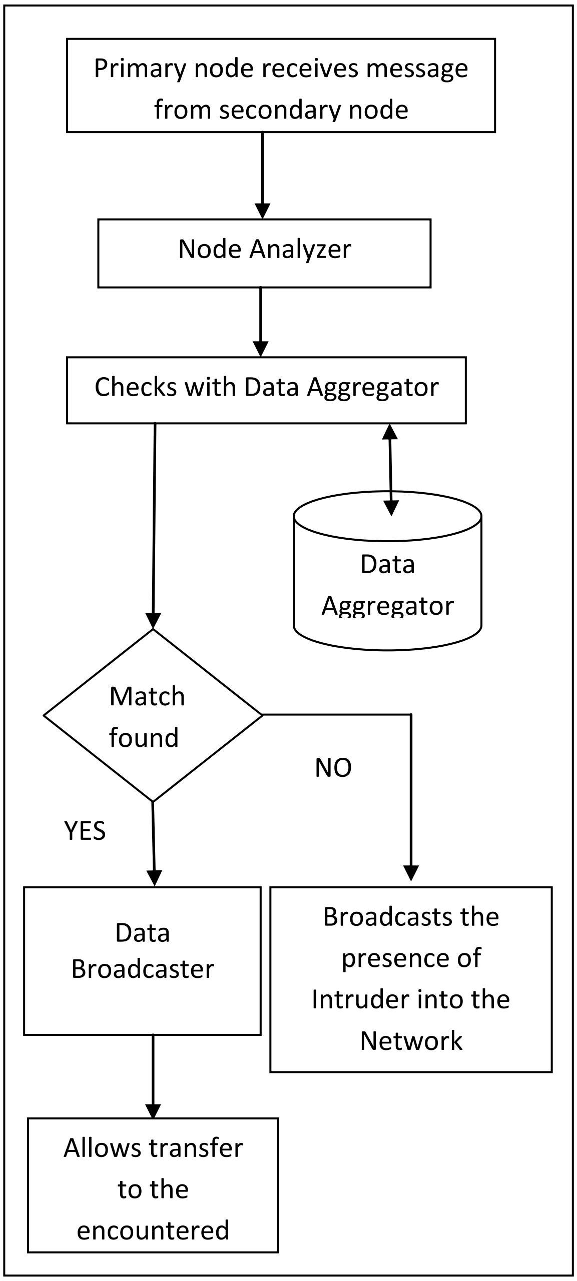
Primary node receives message from secondary node
Node Analyzer
Checks with Data Aggregator
Data Aggregator
Match found
NO
YES
Data Broadcaster
Broadcasts the presence of Intruder into the Network
Allows transfer to the encountered

Fig. 2. Working of Agent

Data Aggregator

The data aggregator is similar to a database that holds an aggregate of information about all the nodes within the network. It includes detailed information of each and every node. The aggregator holds the agent parameters of every node. In plain, it is just the collector of information.

Node Analyzer

The node analyzer analyses whether the node that accept the information is a family node i.e. node that belong to the topology. The analysis is based on the agent parameters that are hoarded in the data aggregator. It selects any one of the parameter in a random manner to conclude that the node is a family node. If a malicious node is sensed, the node analyzer broadcasts the presence of intruder.

Data Broadcaster

In the data broadcaster, once after a node is determined to be a family node, it allows the sender or any relay node to transfer the message packet to the secondary relay node. It acts as a gateway that provides access for communication amidst the encountered nodes.

From Fig. 2 the architecture and working of agent set at each node. When a secondary node receives a message packet from a primary node, the node analyzer analysis whether the node belong to the restricted network. The node analyzer selects one of the parameters randomly and checks for the authorized node from the data aggregator.

The data aggregator is a database, if a match is found within the data aggregator; it is preceded towards the data broadcaster. If the node is not valid, node analyzer broadcasts the presence of the intruder within the network. The data broadcaster allows the node to transfer the message packet to the encountered node.

C. *AES Algorithm*

The AES algorithm is chosen mainly due to its reliable characteristics of security, cost and code compactness and its design and implementation simplicity. As AES [33] accepts data block size of 128, 192, 256 and a key size of 128 bits, which can be variably expanded, it can accommodate a wide spectrum of security strengths for various application needs. Multiple encryptions use a plural number of keys, since it's been avoided in AES, a reduction on number of cryptographic keys for an application to manage is reduced and hence the design of security protocols and systems are simplified.

Initially the input block is converted to a state array of 4 x 4 matrixes, which is of the form described below.

$$\text{Input Block=} \begin{pmatrix} i0 & i4 & i8 & i12 \\ i1 & i5 & i9 & i13 \\ i2 & i6 & i10 & i14 \\ i3 & i7 & i11 & i15 \end{pmatrix} \qquad \text{Eq. 3.1}$$

Where i0, i1, i2…i15 is the user providing input data.

The input key is also expanded and forms a 4 x 4 matrix similar to that of the input block. Based on the input size, the total number of rounds for encryption and decryption may be 10, 12 or 14 with respect to 128, 192 and 256 respectively. Each round excluding the final round involves four transformations for encryption namely

i. Substitute Bytes
ii. Shift Rows
iii. Mix Columns
iv. Add Round Key

The internal functions in AES uphold its operation on a finite field, the polynomials modulo over f(x) [34].

$$f(x) = x^8+x^4+x^3+x+1 \qquad \text{Eq. 3.2}$$

Substitute Bytes

A scheme of non – linear substitution on each byte of the state array is the substitution bytes. It uses an S- box (a lookup table with values) to map the values, it is called a table lookup method. Any non-zero byte x [34] is substituted by the following transformation.

$$Y = Ax^{-1} + b \qquad \text{Eq. 3.3}$$

where A and b are constant 8 x 8 matrixes.

Shift Rows

This operation is actually a transposition cipher. This function operates on each row of a state array [34]. It only rearranges the positions of the element without changing their identities. For elements of ith row, the position rearrangement is cyclic shift to right by 4 – i positions. The transformation is done as follows:

$$\begin{pmatrix} S0,0 & S0,1 & S0,2 & S0,3 \\ S1,0 & S1,1 & S1,2 & S1,3 \\ S2,0 & S2,1 & S2,2 & S2,3 \\ S3,0 & S3,1 & S3,2 & S3,3 \end{pmatrix}$$

$$\downarrow \qquad \text{Eq. 3.4}$$

$$\begin{pmatrix} S0,0 & S0,1 & S0,2 & S0,3 \\ S1,1 & S1,2 & S1,3 & S1,0 \\ S2,2 & S2,3 & S2,0 & S2,1 \\ S3,3 & S3,0 & S3,1 & S3,2 \end{pmatrix}$$

Mix Columns

Mix Columns operates on each column individually. Each byte of a column is mapped into a new value that is a function of all the four bytes of that column. The transformation is done by the matrix multiplication of a state matrix with a constant matrix as follows.

$$C.S = S' \qquad \text{Eq. 3.5}$$

Where S = 4 x 4 matrix before transmission of Eq. 3.4
S' = Outcome f Eq. 35
C = Constant matrix

$$C = \begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \qquad \text{Eq . 3.6}$$

The transformation [33] on any single column j of a state array is as follows.

$$\begin{aligned} S'0,j &= (2.S0,j) \oplus (3.S1,j) \oplus S2,j \oplus S3,j \\ S'1,j &= S0,j \oplus (2.S1,j) \oplus (3.S2,j) \oplus S3.j \\ S'2,j &= S0,j \oplus S1,j \oplus (2.S2,j) \oplus (3.S3,j) \qquad \text{Eq. 3.7} \\ S'3,j &= (3.S0,j) \oplus S1,j \oplus S2,j \oplus (2.S3,j) \end{aligned}$$

Add Round Key

In this transformation, a bitwise XOR [33] operation is done between the elements of the state array and those that of the round key.

The decryption involves four transformations as encryption excluding the final round, but all the functions are invertible. The encryption is inverted in the reverse direction for encryption.

Key Expansion

The key expansion [33] involves expanding the 128 bit key given. It involves the following sequence of three steps.

i. One-byte circular shift on a word.
ii. A byte substitution on each byte of its input using S-box.
iii. The results of previous steps are XOR ed with a round constant RC[j].

$$RC[j] = (RC[j], 0, 0, 0) \qquad \text{Eq. 3.8}$$
$$RC[1] = 1; RC[j] = 2. RC[j-1]$$

IV. Routing Methodology

In this section a secure communication with the aid of B-LoDiS described. An agent is set at each node. During routing, when a sender node A, wishes to transmit a data to a destination node X, it initially send it to a relay node R1 if destination node is not found to be within its boundary.

Node A sends the data only if it confirms that node R1 is a trusted node within the network i.e. it is a node belonging to that particular network. The confirmation on trusted node is done using the agent technology. The agent present at each node generates a test towards R1. The node analyzer of agent at A selects one of the test parameters of agent and passes it to R1. If R1 replies with the correct reply, it is assured to be the trusted node and A passes data towards it. The data actually resides in an encrypted form and sent to R1. R1 just delivers it to another node either relay node Rx (x = 2, 3 ...n) or destination node X. The encryption and decryption is done by AES algorithm.

The selections of the relay nodes are done with the help of Bee routing scheme using objective value (OV). Each node in the network acts as an artificial bee. Initially the bees (here ant refers to the node in the network) will be in the sleep mode and the OV is set to 0. As a data packet is generated at a node A, it searches the relay node in a random manner. The search of relay node is a step of forward phase. The efficiency of the relay node i.e. capability of the relay node to deliver data packet towards destination is determined using the OV estimated during the backward phase and the gossiping method. The gossiping is mainly used to have knowledge about the positions of node in the network to transfer data through it. With the successful delivery of data packet by the relay node, the OV value is incremented each time and the efficiency of the path is shared during the backward phase. LoDiS of B-LoDiS aids in routing by means of the gossiping technique by which each node can determine the location about its immediate nodes. Hence the destination can be reached by Bee routing in aid with LoDiS technique. The routing operates at milliseconds whereas the agent operates at nanoseconds and hence the delay in performing the authentication process will be maintained at an ordinal form. This ensures no degradation in the performance of routing. The pseudocode for secured B-R is depicted in Fig. 3 and the B-R is shown in Fig. 4.

V. Simulation Results

This section describes the simulation results of B-LoDiS with the setup of agent ensuring secure data transmission at each node encounter. The B-LoDiS routing protocol with agent has been evaluated using one simulator [21]. The ultimate motto of B-LoDiS with Agent AES (B-RA) is to enable higher degree of secure communication without degrading the performance of normal routing. Hence B-RA is compared with Epidemic Routing (ER), Spray and Wait (SNW). Since ER is the traditional routing and SNW has optimal performance results of ICMANET, they are compared with B-RA to show off its better results. Section V-A clearly shows the scenario setup for the B-RA. The performance of B-RA is elucidated in the Section V-B. Subsequent to these is the Section V-C performance comparison of B-RA in contrast to ER and SNW are shown.

A. Scenario Setup

The parameters set are the basic one simulator [22] environ parameters and are given in Table 1.

TABLE 1
BASIC SIMULATION PARAMETERS

PARAMETERS	One Simulator
Area	2000 x 2000 m
Mobility Model	Pheromone
Node Density	200 nodes
Node Speed	1.5 m/s
Radio Range	250 m
Packet Life Time	600 s

The one simulation [23-24] for B-R, in this paper, uses the pheromone mobility model. The nodes move in an area of 2000 x 2000 m with a speed limit within bounds 0.5 to 1.5 m/s. The radio range is set to 250 m. The efficiency of any routing protocol is determined by the node density i.e. the total number of nodes within the set network. The packets are generally generated with the initial setup of the simulation and holds through the overall simulation time. The Time To Live (TTL) or the packet life time is set as 600s initially that are varied lately on consideration to the performance criterion. When evaluating, the simulation is run for 3000s.

```
At Source node,
   Choose the destination node using B-R
   Perform the authentication mechanism with the node
encountered
   Encrypt the data pkt using AES algorithm and broadcast it
   Initialize a timer value for rebroadcasting the data pkt

At Destination node,
   Decipher the received pkt by AES decryption mechanism
   If pkt is received for the first time
       Deliver the pkt
   Transmit ack pkt

At Relay nodes,
   Check whether sender is trusted node
    // done by means of agent test parameters
   Update information at encountered node
    // done by means of gossiping technique
```

Fig. 3 Pseudocode of secure B-R

```
Initialize
   OV=0;
Repeat
   For all nodes
      Bee_Route();
Until route found
Bee_Route()
   If no route found
      Fwd_phase() //search for relay nodes
   End if
   If route found
      Bwd_phase()//estimate the path using OV
         OV+=1;
   End if
   For OV=max
      Deliver data packet
End Bee_Route()
```

Fig. 4 Pseudocode for B-R

B. Performance of B-RA

On setting of agent the performance to route packets in ICMANET should not degrade. As setting of agents eventually decreases the time complexity i.e. it decreases the time required to route packet. The agent setup ensures a higher scale of security. These general properties of Agent along with B-R, endow with a secure communication or transfer of message packets across the network. In this work, we simulated an optimal result with agent setup at each node. Data transmission is done with data encryption-decryption techniques using AES cryptographic algorithm ensuring higher authentication during communication.

The performance of any routing protocol is assessed by the node density, node speed, its life time in disparity to which the overhead, number of transmissions, delivery ratio and delay are to be maintained optimal. The setting of agent provides high security. In this work, we show a better performance amidst these concerns.

To evaluate performance, the various network parameters were evaluated by varying the number of nodes and a node's transmission range.

C. Performance Comparison of B-RA with ER and SNW

To show the pro of B-RA, we compared the simulated result of B-RA with ER and SNW. In order to mark the performance of B-RA, a comparative analysis is made between the above mentioned three protocols.

We have made the comparison using various metrics as follows:

i. Performance with respect to Delivery Ratio
ii. Performance with respect to Overhead
iii. Performance with respect to Delivery Latency
iv. Performance with respect to Malicious Nodes

To show the effect of secured routing in B-RA, it is measured with number of malicious nodes isolated from the network as well as number of packets routed through malicious nodes. These two are evaluated with respect to mobility and number of nodes in the network.

Performance with respect to Delivery Ratio

Comparing the delivery ratio i.e. the probability to deliver the message, B-RA shows a maximum delivery rate in contrast to ER and SNW. The comparative results are shown in Fig. 5 and Fig. 6 varying the number of nodes and the transmission range respectively.

ER incurs minimum delivery rate when compared to SNW and B-RA whereas delivery rate is at a maximum rate in B-RA. The ratio of delivery rate is lesser in ER and SNW when compared to B-RA is mainly due to the non effective usage of intermediate nodes. In ER the forwarding of data is by means of pair-wise connectivity between nodes.

As the probability of connecting nodes pair-wise is less, its delivery rate is low. Whereas SNW forwards through node mobility through spraying mechanism resulting the probability to reach destination varies. Hence has lesser delivery rate than B-RA. B-RA uses the immediate intermediate nodes that it encounters during node mobility hence has higher delivery rate than ER and SNW. It is mainly due to the fact that B-RA has higher probability of reaching the destination than ER and SNW. Along with higher delivery rate B-RA ensures soaring secure communication. The authentication terminologies do not degrade the normal routing performance.

Performance with respect to Overhead

The overhead remains a major network parameter need to be considered to evaluate the performance. B-RA has a constant overhead at all conditions. Fig. 7 and Fig. 8 shows the variation of B-RA, ER and ER with respect to number of nodes and transmission range respectively.

ER has higher overhead as it involves pair-wise connectivity for routing. Since the connectivity between same nodes is possibly frequent, the ratio of overhead is higher. SNW shows a constant overhead upto a certain range and it slightly increases as the load and radio range gets increased. It is mainly due to the fact that during wait phase SNW has to wait indefinitely to meet up with the destination node. In B-RA the overhead is constant for all varying load and radio range of a node. Since in B-RA the transmissions are bound to the packets generated at each node, overhead remains constant. With this B-RA assures secure communication.

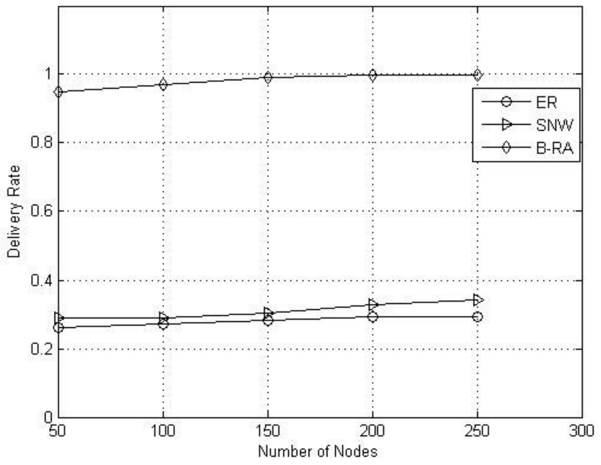

Fig. 5. Delivery Ratio for various numbers of nodes

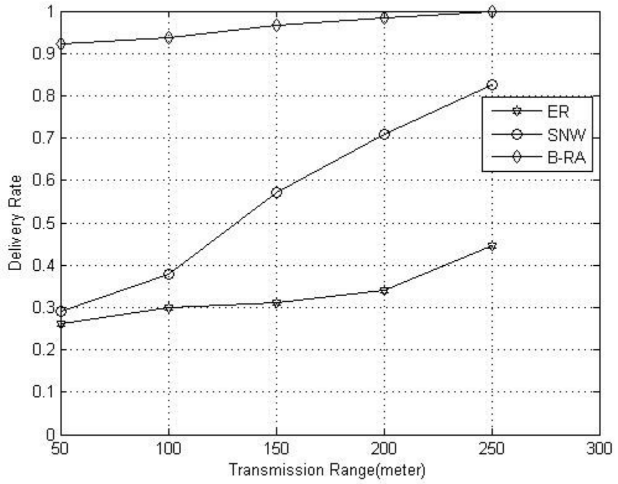

Fig. 6. Delivery Ratio with varying transmission range

Performance with respect to Delivery Latency

The time criteria once again stand forth as an important aspect during the measure of latency. The delay in delivering the data packets towards the destined node is lesser in B-RA. Fig. 10 and Fig. 11 show the variation of B-RA, ER and ER with respect to number of nodes and transmission range respectively.

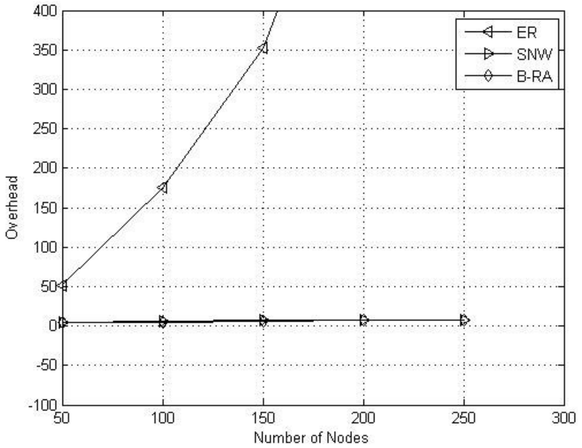

Fig. 7. Overhead for assorted number of nodes.

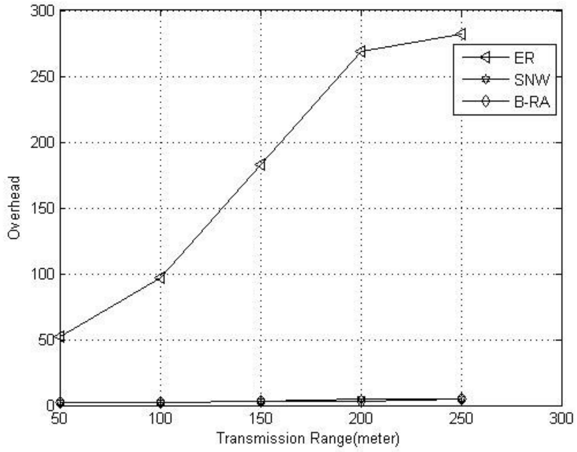

Fig. 8. Overhead by varying transmission range

The delay in delivering the data packets towards the destination is larger when compared to SNW and B-RA. The pair-wise connectivity between nodes in the network does not ascertain higher probability to reach the destination in minimum time period. SNW has an optimal delay; it is mainly due to the imprecise time by a node to reach the destination. B-RA incurs minimum delay as the nodes are capable of reaching the destination through location services. The nodes are not in need to wait for any beacons and any node is destined to reach the destination. Hence the delay is lesser with secure data transmission.

Performance with respect to Malicious Nodes

The secure routing through B-RA is evaluated with number of malicious nodes isolated from network and the number of packets routed through such malicious nodes. The isolated malicious nodes form network depicts the potency of secure routing scheme with detection of intruders in to the network. The fig. 11 and fig. 12 portray the possibility of B-RA to detect the malicious node in the network at higher rate. It is mainly due to the fact that B-RA uses the authentication terminologies. When a node fails to meet the authentication terminologies, it is suspect to be a malicious node in the network. In ER and SNW, the possibility to detect the malicious node is less as they rely truly on the intermediate nodes they encounter during transmission. As they immediately transfer the data packet when they encounter their rely node. When the number of nodes is increased in the network, more malicious nodes are detected as it uses a gossiping process for authentication. Whereas ER and SNW due to the absence of sharing scheme, detection of malicious nodes becomes arduous.

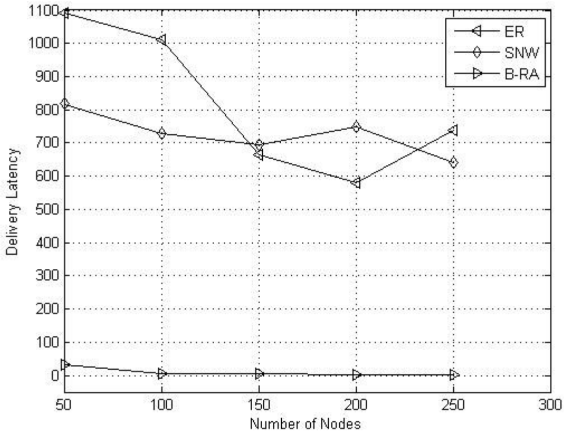

Fig. 9. Delivery Latency for assorted number of nodes.

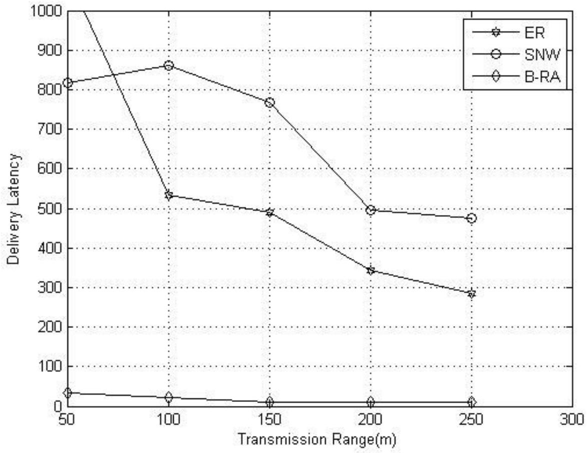

Fig. 10. Delivery Latency with varying transmission range.

Considering the fact of number of packets routed through the malicious node, the probability of routing across malicious node is found to be less in B-RA compared to ER and SNW. It is clearly depicted in fig. 13 and fig. 14 respectively. The lesser transmission of packets through malicious nodes is mainly due to the efficient detection of malicious nodes by B-RA which is absent in ER and SNW.

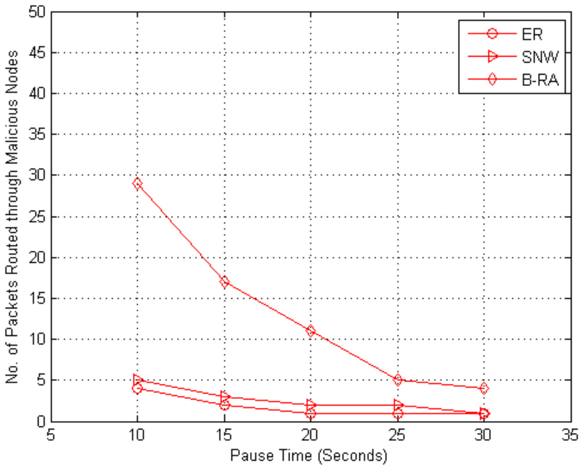

Fig. 11. Number of Malicious Nodes Isolated with respect to Mobility

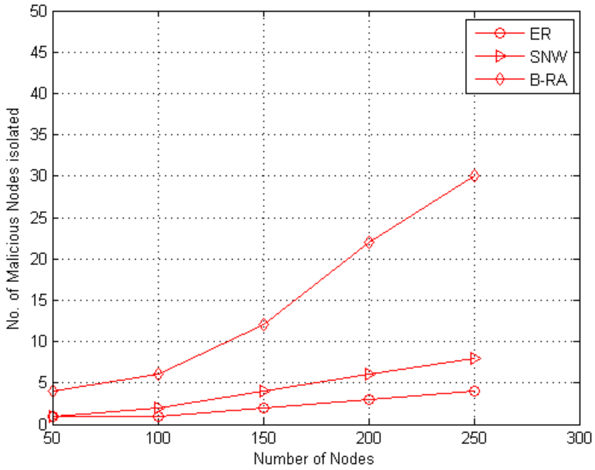

Fig. 12. Number of Malicious Nodes Isolated with respect to Number of Nodes

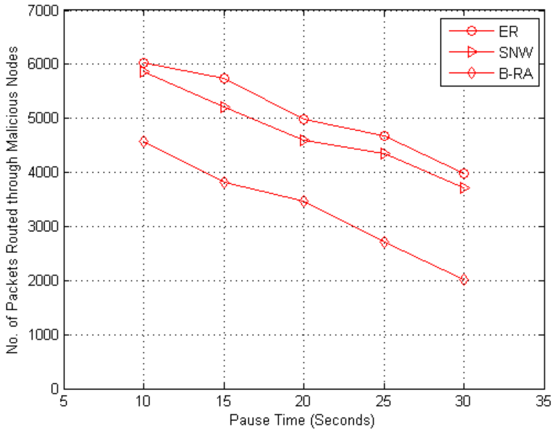

Fig. 13. Number of Packets Routed through Malicious Nodes with respect to Mobility

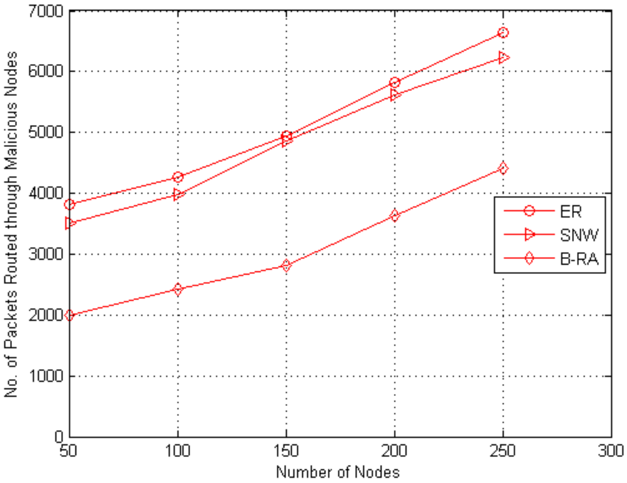

Fig. 14. Number of Packets Routed through Malicious Nodes with respect to Number of Nodes

Thus these metrics clearly show that B-RA is an efficient protocol for secure routing in ICMN.

Thus these metrics clearly show that B-RA is an efficient protocol for secure routing in ICMN. The proposed B-LoDiS is capable of defending the below mentioned attacks [41].

i. **Dropping Data Packets:** this denial of service attack is detected as the malicious nodes do not answer the query posed by agent at each node.
ii. **Dropping Control Packets:** this denial of service attack is detected as the malicious node does not route the data packet as it fails to answer the query generated by agent at each node.
iii. **Flooding:** as each node determines its immediate relay node to transmit data, the possibility to flood the agent queries is impractical.
iv. **Gray hole:** as agent queries and information regarding the relay nodes are updated periodically, this attack will be detected.
v. **Spoofing:** through the answer verification scheme of agent technology, one cannot spoof to be other, since the same answer cannot be generated. Hence this attack is detected.

CONCLUSION

In this paper, we have demonstrated the means of secure node communication and data transmission in ICMANET. The authentication terminologies set at each node is assured by agent technology. The agent parameters aid in detecting the possibility of intruders in the network. The secure data transmission between nodes is possible with the cryptographic technique AES. With all these intruder detecting policies, the normal routing performances are not degraded. B-RA similar to LLR achieves maximum delivery rate, minimum delay and constant overhead. B-RA with superior performance ensures scalable security. The possibilities of threats and malicious attacks are controlled in B-RA. On setting agent this protocol ensures a secure delivery of the message packets. It is evident from this that the basic properties of LLR protocol like fewer transmissions, low contention, better delivery delay and high scalability are achieved with a generalised value. A comparative analytic and simulative result of B-RA with ER and SNW are roofed in this paper. This paper, in general ensures secure communication without any performance degradation. This paper proves secure routing with agent technology and cryptographic mechanisms. This paper proves secure routing with agent technology and cryptographic mechanisms and is tested with the malicious nodes.

REFERENCES

[1] Erik Kuiper and Simin Nadim-Tehrani, “ Geographical Routing with Location Services in Intermittently Connected MANETs”, IEEE Trans. Veh. Technol. Vol. 60, no. 2, pp. 592 – 694, Feb. 2011.

[2] T.Spyropoulos, K. Psounis, and C. S. Raghavendra, “Spray and Wait :An Efficient Routing Scheme for Intermittently Connected Mobile Networks,” in Proc. ACMSIGCOMM Workshop Delay – Tolerant Netw., 2005, pp. 252-253.

[3] W. K. Lai, W. K. Chung, J. B. Tsai, and C. S. Shieh, “Spray and Hop: Efficient Utility–Mobility Routing for Intermittently Connected Mobile Networks,” in Proc. Int. Conf. Comput. Commun., Chinacom., 2009.

[4] E. J. Jebajothi, V. Kavitha, and T. Kavitha, “Contention Based Routing in Mobile Ad Hoc Networks with Multiple Copies,” in Int. Journal of Engg. and Technol., vol. 2, 2010, pp. 93-96.

[5] K. Shi, “Semi-Probablistic Routing in Intermittently Connected Mobile Ad-Hoc Networks,” in Journal of Info. Science and Engg.,vol. 26, 2010, pp. 1677-1693.

[6] T. Spyropoulos, K. Psounis, and C. Ragavendra, “Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case,” IEEE/ACM Trans. Netw., vol. 16, no. 1, pp. 77-90, Feb.2008.

[7] T. Spyropoulos, K. Psounis, and C. S. Ragavendra, “Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case,” IEEE/ACM Trans. Netw., vol. 16, no. 1, pp. 63–76, Feb. 2008.

[8] Z. Li, and H. Shen, “A Direction Based Geographic Routing Scheme for Intermittently Connected Mobile Networks,” in IEEE/IFIP Int., Conf.,Embedded and Ubiquitous Computing, 2008, pp. 359-365.

[9] J. Ghosh, H. Q. Ngo, and C. Oiao, “Mobility Profile based Routing within Intermittently Connected Mobile Ad Hoc Networks,” in Proc. ACM Wireless Commn., and Mobile Computing, 2006, pp. 551-556.

[10] R. R. Choudhury, “Brownian gossip: Exploiting Node Mobility to Diffuse Information in Ad Hoc Networks,” in Proc. Int. Conf. CoA-LAborative Comput.: Netw., Appl. Worksharing, 2005, pp. 1-5.

[11] M. Musolesi, S. Hailes, and C. Mascolo, “Adaptive Routing for Intermittently Connected Mobile Ad Hoc Networks,” in Proc.IEEE6th. Int. Symposium, WoWMoM, 2005.

[12] M. Heissenbüttel, T. Braun, T. Bernoulli, and M. Wälchi, “BLR: Beaconless Routing Algorithm for Mobile Ad Hoc Networks,”, Comput. Commun., vol. 27, no. 11, pp. 1076-1088, Jul. 2004.

[13] A. Vahdat and D. Becker, “Epidemic Routing for Partially Connected Ad Hoc Networks,” Duke Univ., Duhram, NC, TecH.Rep. CS-2000-06, 2000.

[14] J. Ghosh, C. Westphal, H. Ngo, and C. Qiao, “Bridging Intermittently Connected Mobile Ad Hoc Networks (ICMAN) with Sociological Orbits.”

[15] D. Cokuslu, K. Erciyes, “A Flooding based Routing Algorithm for Mobile Ad Hoc Networks,” in IEEE 16th. Int. Conf. SIU 2008, pp. 1-5.

[16] Islam M. Hegazy, Taha Al-Arif, Zaki.T. and Hossam M. Faheem,”A Multi-Agent Based System for Intrusion Detection”, IEEE Potentials, 2003.

[17] L. Beson and P. Lelar, “A Distributed Intrusion Detection System for Ad Hoc Wireless Sensor Networks. The AWISSENET Distributed Intrusion Detection System”, in IEEE, 2009.

[18] K. Ioannis, T. Dimitriou, F. C. Freiling, “Towards Intrusion Detection in Wireless Sensor Networks”, in 13th European Wireless Conference, Paris, Apr. 1997.

[19] Ioanna Stamouli, “Real-time Intrusion Detection for Ad-hoc Networks”, Master of Science dissertation, University of Dublin, 2003.

[20] O. Kachirski, R. Guba, D. Schwartz, S. Stoecklin and E. Yilmaz, “Casebased Agents for Packet-Level Intrusion Detection in Ad-hoc Networks”, in Proceedings of the 17th International Symposium on Computer and Information Sciences, CRC Press, Oct. 2002, pp. 315-320.

[21] A. Keranen, J. Ott and T. Karkkainen, “The One Simulator for DTN Protocol Evaluation”, in ICST.

[22] A. Keranen, T. Karkkainen and J. Ott, “Simulating Mobility and DTNs with the ONE”, Jour. Of Commun., vol.5, no.2, Feb 2010.

[23] A. Keranen, “Opportunistic Network Environment Simulator”, Special Assignment report, Helsinki University of Technology, Department of Communications and Networking, May 2008.

[24] TKK/COMNET. Project page of the ONE simulator. http://www.netlab.tkk.fi/tutkimus/dtn/theone, 2009.

[25] F. Yin, X. Yin, Y. Han, L. He, H. Wang, “An Improved Intrusion Detection Method in Mobile AdHoc Network”, IEEE, 8th Int. Conf. Dependable, Automatic and Secure Computing,

2009, pp. 527-532.

[26] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan, “Enhanced Intrusion Detection Techniques for Mobile Adhoc Networks”, IET-UK ICTES, Dec 2007, pp. 1008-1013.

[27] I. Stamouli, P. G. Argyroudis and H. Tewari, “Real-Time Intrusion Detection for Ad hoc Networks”, IEEE, WoWMoM, 2005.

[28] S. Bose, S. Bharathimurugan and A.Kannan, “Multi-Layered Integrated Anomaly Intrusion Detection System for Mobile Adhoc Networks”, IEEE-ICSCN, 2007.

[29] K. Samad, E. Ahmed, W. Mohamood, K. Sharif, A.A. Chaudhry, “Efficient Clustering Approach for Intrusion Detection Ad Hoc Networks”.

[30] A. F. Farhan, D. Zulkhairi, M. T. Hatim, “Mobile Agent Intrusion Detection System for Mobile Ad Hoc Networks: A Non-overlapping Zone Approach”, IEEE, 2008.

[31] H. Otrok, M. Debbabi, C. Assi and P. Bhattacharya, “A Cooperative Approach for Analyzing Intrusions in Mobile Ad hoc Networks”, IEEE, ICDCSW’07, 2007.

[32] S. Ramesh, R. Indira, R. Praveen and P. Ganesh Kumar, “Agent Technology for Secure routing in Intermittently Connected MANETs”, in the Proceedings of the National conference on Recent Advances in Computer Vision and Information Technology (NCVIT’13), 2013.

[33] William Stallings, “Cryptography and Network Security, Principles and Practices”, Fourth Edition, Pearson Education.

[34] Wenbo Mow, “Modern Cryptography, Theory and Practice”, Fourth Edition, Pearson Education.

[35] Dusan Teodorovic, “Bee Colony Optimization (BCO)”, University of Belgrade, Faculty of Transport and Traffic Engineering, Vojvode Stepe 305.

[36] Li-Pei Wong, Malcom Yoke Hean Low, Chin Soon Chong, “Bee Colony Optimization with Local Search for Travelling Salesman Problem”, pp. 1019-1025.

[37] Li-Pei Wong, Malcom Yoke Hean Low, Chin Soon Chong, “An Efficient Bee Colony Optimization Algorithm for Travelling Salesman Problem using Frequency-based Pruning”, 7th International Conf. on Industrial Informatics (INDIN), IEEE, 2009, pp. 775-782.

[38] M.H. Saffari, M.J. Mahjoob, “Bee Colony Algorithm for Real-Time Optimal Path Planning of Mobile Robots”, IEEE, 2009, pp. 1-4.

[39] M.A. Rahim, I. Musirin, I.Z. Abidin, M.M. Othman, D. Joshi, “Congestion Management Based Optimization Technique using Bee Colony”, 4th InternationalPower Engineering and Optimization Conference (PEOCO2010), June 2010, pp. 184-186.

[40] Li-Pei Wong, Malcom Yoke Hean Low, Chin Soon Chong, “A Bee Colony Optimization Algorithm for Travelling Salesman Problem”, IEEE, 2nd International Conf. on Modelling and Simulation, 2008, pp. 818-823.

[41] S. K. Dhurandher, M. S. Obaidat, K. Verma, P. Gupta, and P. Dhurandher, FACES: Friend – Based Ad Hoc Routing using Challenges to Establish security in MANETSs systems. IEEE Sys. Jour., vol. 5, no. 2, pp. 176-188, Jun. 2011.

[42] Sekaran and Parasuraman, A Secure 3-Way Routing Protocol for Intermittently Connected Mobile Adhoc Networks, *The Scientific Journal, Vol 2014, Article ID 865071*, Hindawi Publishing Corporation. http://dx.doi.org/10.1155/2014/865071