Trends in Applied Sciences Research

ISSN 1819-3579

Academic
Journals Inc.

www.academicjournals.com

Trends in Applied Sciences Research 7 (11): 881-900, 2012
ISSN 1819-3579 / DOI: 10.3923/tasr.2012.881.900

EMNet: Electromagnetic-like Mechanism based Routing Protocol for Mobile *Ad Hoc* Networks

[1,2]S.K. Tiong, [1]H.Sh. Jassim, [3]S.Yussof, [1]S.P. Koh and [4]David F.W. Yap
[1]Center of System and Machine Intelligence, [2]Power Engineering Center, [3]College of Information Technology, Universiti Tenaga Nasional, 7 km, Jalan Ikram-Uniten,43000 Kajang, Selangor, Malaysia
[4]Faculty of Electronics and Computer Engineering, Universiti Teknikal Malaysia Melaka, Hang Tuah Jaya, 76109 Durian Tunggal, Melaka, Malaysia

Corresponding Author: H.Sh. Jassim, Center of System and Machine Intelligence, College of Information Technology, Universiti Tenaga Nasional, 7 km, Jalan Ikram-Uniten,43000 Kajang

ABSTRACT

A mobile *ad-hoc* network (MANET) is a collection of mobile nodes without any specific fixed infrastructure. The connectivity among the nodes may differ with time due to nodes are randomly moving and may join or leave the network at any time. Hence, an efficient routing protocol is needed to allow communication over dynamic MANET topology. Several *ad hoc* routing protocols have been proposed and implemented to determine the most efficient path to route information through dynamic nodes in MANET. Meanwhile, due to most of the mobile nodes have different Quality of Service (QoS) requirements, recent research work of MANET routing has focused on developing protocol that is able to support various QoS requirements. In this study, a new routing protocol namely EMNet has been proposed to cater for different QoS requirements in MANET. It was designed based on an artificial intelligent technique namely Electromagnetic-like Mechanism (EM), which simulating the attraction-repulsion mechanism theory of electromagnetism. The EM generated solutions for new path establishment and broken links restoration by regenerating new individuals with quality improvement through its attraction-repulsion process. The new EMNet protocol has been simulated in various MANET scenarios and its performance in routing was compared with conventional *ad-hoc* On-demand Distance Vector (AODV) routing protocol. The simulation results show that EMNet is able to achieve better results in terms of packet delivery, normalized routing load, end-to-end delay, overhead, and throughput in comparison with AODV in the simulation scenarios.

Key words: Component, mobile *ad-hoc* network, routing protocol, electromagnetic-like mechanism (EM), dynamic unicast

INTRODUCTION

Mobile *ad-hoc* network (MANET) is a collection of mobile nodes that do not have fixed infrastructure or any centralized controller such as access point or server to determine the route of the paths. Each node in an *ad hoc* network generally relies on each other to forward packets to its destination node. Therefore, an efficient route mechanism is needed for forwarding packets from source to the target destination (Perkins and Royer, 2003). Such devices can communicate with another device that is immediately within their radio range or one that is outside their radio range

without relying on access point or any centralized control. In MANET, mobile nodes can join and leave the network at anytime and free to move randomly. MANET systems are suitable to be used in scenarios such as a battlefield, an emergency operation, conference halls and disaster relief (Rajabhushanam and Kathirvel, 2011).

One of the main characteristics of these networks is its dynamic topology. Since nodes in the network can move arbitrarily, the topology of the network also changes frequently. Furthermore, the bandwidth of the link is constrained and the capacity of the network also varies tremendously. Due to the dynamic topology, the output of each relay node will vary with the time. Power limitation in mobile devices is an essential factor. Generally, node in MANET uses battery as their power supply. Thus, advanced power conservation techniques are greatly needed in designing a system. Besides that, the mobile network security is also physically limited causing it to be easily attacked compared to the fixed network (Milanovic and Malek, 2004).

The main aim of the existing MANET routing protocols is to find the shortest path in the source-destination routes selection (Buruhanudeen *et al.,* 2007) and discover only a single path from the source to destination. However, recent researchers developed potentially promising approach to establish multiple paths between source and destination. Hence in this study, we aim to develop a new MANET routing algorithm with Electromagnetic-like Mechanism (EM) (Birbil and Fang, 2003) that is able to determine the optimum routing path based on three factors which are trust, power-level and hop count (shortest path). Besides, the new developed routing algorithm is equipped with multiple paths storing capability, specifically for meeting different QoS requirements.

LITERATURE REVIEW

There are a number of *ad hoc* routing protocols that have been proposed and implemented. These protocols can be classified into three categories, namely, proactive, reactive and hybrid. Examples of existing routing protocols for MANET are *Ad-hoc* On-demand Distance Vector (AODV) (Perkins and Royer, 2003), Destination Sequenced Distance Vector (DSDV) (Khan *et al.*, 2008), Dynamic Source Routing (DSR) (Johnson *et al.*, 2007) and *Ad hoc* On-demand Multipath Distance Vector (AOMDV) Routing protocol (Jing *et al.*, 2006).

Li *et al.* (2004) used Trust *Ad hoc* On-demand Distance Vector (TAODV) trust metrics for routing decisions and avoid nodes that were not trusted. In the proposed TAODV, the routing messages and routing table of *Ad hoc* On-demand Distance Vector AODV had been extended to include trust information which could be updated by monitoring the behaviors of other nodes in the network. Jassim *et al.* (2009) proposed a new protocol named as Reliant *Ad-hoc* On-demand Distance Vector Routing (R-AODV). In this protocol, AODV was extended by incorporate a trust mechanism known as direct and recommendations trust model. This enables AODV to not only find the shortest path but also find the shortest path that can be trusted. Thus, the security will be enhanced by ensuring that data does not go through malicious nodes that have been known to misbehave. Ghalavand *et al.* (2010) extended AODV was by adding trust and energy power values to the route packet. Fuzzy Logic algorithm was applied to select route with high trust value and energy capacity. However, this work did not put into consideration the routing of the shortest path and it also applies single path routing between source node and distention.

Since, battery power is a critical factor that determines the functionality of mobile *ad hoc* networks, many route selection protocols with a specific goal of achieving energy-efficient routing. Xie *et al.* (2007), the authors try to balance the load among nodes and this has been shown to

maximize the network lifetime. Woo *et al.* (2001) proposed Localized Energy Aware Routing (LEAR) protocol in which the Dynamic Source Routing (DSR) routing protocol was modified for balanced energy consumption. In DSR, when a node receives a route-request message, it appends its identity in the message's header and forwards it toward the destination. Thus, an intermediate node always relay messages if the corresponding route is selected. However, in LEAR, a node determines to forward the route-request message based on its residual battery power (Er). When Er is higher than a threshold value (Thr), the node forwards the route-request message; otherwise, it drops the message and refuses to participate in relaying packets.

Therefore, the destination node will receive a route-request message only when all intermediate nodes along a route have good battery levels and nodes with low battery levels can conserve their battery power.

There are also several routing protocols have been proposed using artificial intelligent techniques. One of the protocols includes the Ant Routing Algorithm for Mobile *Ad-hoc* Networks Based on Adaptive Improvement (ARAAI). Research studies show that ants have the ability to find the shortest path between their nest and the food source (Bonabeau *et al.*, 1999; Broch *et al.*, 1998). The ability is caused by a substance known as pheromone, which is deposited by ants as they move along the path. The concentration of pheromone decreases with time due to diffusion effects. ARAAI adapted the ants' ability in determining the shortest route. Each node in the mobile *ad-hoc* network contains a routing table to record routing information and a neighbor table to maintain local connectivity. The heuristic value is local node energy information collection, and it is used for selecting route in the existing multi-path (Broch *et al.*, 1998). Neighbor table is represented as a connection between local and other nodes. Zeng and He (2005) presented an excellent routing protocol by using the adaptive ant colony algorithm to realize route discovery and make improvement in global searching optimization. However, this technique needs to be enhanced to reduce the route discovery delay and to improve the efficiency and scalability. Rajagopalan and Shen (2006) presented *ad hoc* routing protocol with swarm intelligence (ANSI) which was able to work for hybrid *ad hoc* networks by maintaining the state information about the neighboring network. Proactive ants are periodically emitted to find and maintain routing paths in the vicinity of a node. Reactive forward and BANTs are used if a node needs to find a path to an unknown destination.

Furthermore, Cheng and Yang (2010) adapted several Genetic Algorithms (GA) to solve the dynamic multicast routing problem. They proposed to integrate several immigrant schemes into the GA to enhance its searching capacity of the optimal multicast tree in dynamic environments. Once the topology is changed, the new immigrants can help guide the search of good solutions in the new environment. It could be an excellent idea of finding the optimum path using several GA algorithms; however, it can cause very high percentage of overhead in order to find the optimum path. Besides, the experimental results of this work showed that these immigrants based genetic did not consider the performance of network in term of accuracy and efficiency.

PROPOSED APPROACH AND METHODOLOGY

Trust model representation: The trust model adopted in this study was proposed by Chuanhe *et al.* (2007) called Dynamic Mutual Trust based Routing protocol (DMTR). DMTR is to establish the trustworthy relationship between nodes in MANET. The idea of DMTR was based on Trust Network Connect (TNC) to improve the security of the path selected (Chuanhe *et al.*, 2007).

Trust(u) represents the node u's trust score during the periodical time t. The range of Trust(u) is given as {0≤Trust(u)≥100}, where 0 denotes that the node is untrustworthy, 100 denotes that the node is fully trustworthy.

During the periodical time t, if the transactions between node A and node u is m times, the degree of satisfaction of ith time is S(u,i), S(u,i) ∈ [0, 1]. The value 1 denotes that the node u makes the node A satisfies absolutely. If the value is 0, it denotes that the node u makes the node A dissatisfies absolutely, making the node u to be untrustworthy. Assume that TF(u,i) is the weight of ith transactions.

The direct trust of node u is defined as:

$$\text{Direct}_{\text{Trust}}(u) = \frac{\sum_{i=1}^{m} S(u,i) \times TF(u,i)}{\sum_{i=1}^{m} TF(u,i)} \tag{1}$$

The indirect trust of node u is measured by other nodes' recommendations and is defined as follows:

$$\text{INDirect}_{\text{Trust}}(u) = \frac{\sum_{i=1}^{m} t\ u(i) \times \text{Direct}_{\text{Trust}}(i)}{\sum_{i=1}^{m} \text{Direct}_{\text{Trust}}(i)} \tag{2}$$

$\text{INDirect}_{\text{Trust}}$ (u) represents the indirect trust of node u while t u(i) is the direct trust of node u relative to node i,$\text{Direct}_{\text{Trust}}$ (u) i's direct trust.

The node u trust denotes that:

$$\text{Trust}(u) = \alpha \times \text{Direct}_{(\text{trust})}(u) + \beta \times \text{INDirect}_{(\text{trust})}(u) + \gamma \times \text{Trust}_{l}(u) \tag{3}$$

Trust(u) represents the trust score collected for node u during the time t. The value of α, β, γ which ranges from [0 to 1] are the weight of direct trust, indirect trust and trust score respectively as collected during the time t.

Thus, the trust value of the ith path is:

$$TPi = \Delta - \frac{(\Delta - T_{min})}{T_{min} - \omega} \tag{4}$$

where, Δ is the average trust score of nodes in the path. T_{min} is the minimal trust value in the path. ω is boundary value between the distrust and trust. TPi is the trust value of ith path.

Battery capacity representation: Each node will share its Ei remaining battery capacity with other nodes during the routing discovery process. All nodes has the responsibility to add their remaining battery capacities into the request RREQ packets.

As the RREQ messages are broadcasted, each intermediate node that does not have a route to the destination forwards the RREQ packet after appending its remaining battery capacities into battery capacity accumulator S[E] in the packet which is computed by:

$$\left[S[E] = \sum_{i=1}^{n} E(i) \right] \tag{5}$$

where, n is No. of hop counts received in one path, S[t] is the battery capacity summation accumulator, Ei is temaining battery capacity for node i.

Hence, at any point, the RREQ packet contains a list of all the nodes visited with their battery capacities added into the battery capacity summation accumulator S[E].

Whenever an intermediate node receives a RREQ packet, it will check the updates of the route to the source node. Subsequently, it computes the average of battery capacity for path i by using the equation:

$$\left[(B_{pi}) = \frac{S[E]}{Hc(pi)} \right] \tag{6}$$

Hop count representation: Hop count is the number of hops from the Originator IP Address to the node handling the request. In other words, $Hc(p_i)$ is the total of hop count from the source to the destination in path i . This criteria eventually helps routing protocols to select the shortest path:

$$Hc(p_i) \in \{0 = Hc(p_i) \geq \infty\} \tag{7}$$

$$Hc(p_i) = \begin{Bmatrix} 0 & \text{Beforbroadcastingthe PREQ} \\ 1 & \text{If the destination is the next hop} \end{Bmatrix} \tag{8}$$

Design of electromagnetic-like mechanism based on different quality of service qos: Electromagnetic-like mechanism (Birbil and Fang, 2003) is a population based algorithm which simulates the attraction-repulsion mechanism of the theory of electromagnetism. Each individual in the population is called as particle of solution, which represent the sample point in the search space. Each particle is associated with charge with its objective function value and its strength determines the magnitude of attraction or repulsion of the point over the sample population. The better the objective function value, the higher the magnitude of attraction. The attraction directs the points toward better regions, whereas repulsion allows particles to exploit the unvisited regions.

The electromagnetic-like mechanism begins with a population of solutions which are randomly generated, whereby each solution represents one path. EM will then iteratively improve the solution by applying a great deluge algorithm. The main reason that the Standard Electromagnetic-like Mechanism SEM cannot work properly in discrete space problems is due to its operators (force calculation and movement) incompatibility. Great deluge is a local search procedure that allows the worst solutions to be accepted based on some given upper boundary.

Initially, the charge of each particle is calculated. The static force between two point charges is proportional to the magnitude of the charges and inversely proportional to the square of the distance between the charges (Birbil and Fang, 2003). The fixed charge of path i is calculated as:

$$q^i = \exp\left(-n \frac{f(x^i) - f(x^{best})}{\sum_{k=1}^{m} f(x^k) - f(x^{best}))} \right) \tag{9}$$

Where:

q^i	=	The charge for path i
$f(x^i)$	=	Penalty of path i
$f(x^k)$	=	Penalty of path k
$f(x^b)$	=	Penalty of path b (b = best path through population)
m	=	Population size
n	=	No. of paths

The solution quality or charge of each path determines the magnitude of an attraction and repulsion effect in the population. A better solution encourages other particles to converge to attractive valleys while a bad solution discourages particles to move toward this region. These particles move along with the total force and thus, diversified solutions are generated. The total force of particle i is calculated as:

$$F_{ij} = \sum_{j \neq i}^{m} \left\{ \begin{array}{l} (f(x^j) - (f(x^i)) \dfrac{q^i q^j}{\left\| f(x^j) - f(x^i) \right\|^2} \text{ if } f(x^j) < f(x^i) \\ (f(x^i) - (f(x^j)) \dfrac{q^i q^j}{\left\| f(x^j) - f(x^i) \right\|^2} \end{array} \right\}, \forall i \tag{10}$$

In general, the process of evaluating the total force is as illustrated in Fig. 1. Three particles labeled as 1, 2 and 3, are represented as feasible solutions with their associated objective function value of 45.78, 43.81 and 39.50 respectively. Since particle 1 is worst than particle 3, a repulsive force F_{13} effects on particle 1. Particle 2 is better than particle 3, thus an attractive force F_{23} effects on particle 3 causing the attraction-repulsive force in different directions.

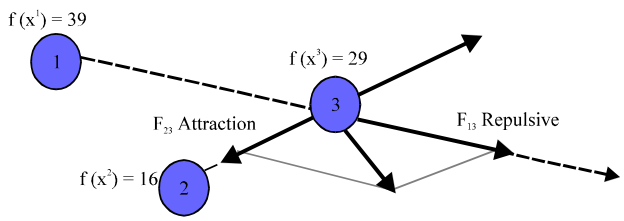


Fig. 1: Attraction-repulsive effect on particle 3

PROBLEMS FORMULATION

We consider a MANET unicasting within the input of the shortest path problem can be stated as follows:

s	=	The source node of unicasting request.
d	=	The destination node received the unicast request.
Ti (UTi , Nti)	=	A unicast tree with nodes UTi and links NTi
PTi (s, dj)	=	A path from s to d on the tree Ti.
B_{pi}	=	The average of battery capacity for ith path on Ti tree.
Tp_i	=	The trust value of the ith path of the tree Ti.
Hc(pi)	=	The total hop counts on the path Pi (i =1,... ,N).

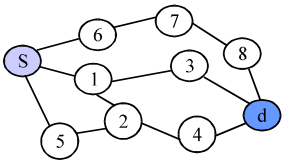
In this problem, an objective function is developed which satisfy the hop count with the cost as shown in Eq. 11:

$$\text{Max}\left\{\frac{\sum_{Ti\in P_T^{(s,dj)}} TP_i \cdot \sum_{Ti\in P_T^{(s,dj)}} B_{pi}}{\sqrt{Hc(p_i)}}\right\} \tag{11}$$

Solution representation: A unicast tree is a collection of neighbors nodes from the source to each destination on the tree. Hence, a routing path has information about sources, destination nodes and IDs of nodes which the path passes. This information can be organized as following:

- The Source IP Addr contains IP address of originator node
- The Sequence Number is the local counter maintained by each node and incremented each time when RREQs are generated by source
- The Dest IP Addr generally contains IP address of destination node
- The trust score is the trust value of node i in path i
- Indirect trust is the recommendation trust value for node i
- Battery capacity accumulator the average of battery capacity for ith path on the tree Ti

The solution is represented as one path that contains of an array. Each cell represents the node IDs and the length of the array should not exceed the number of nodes in the network. Since there is a number of routing tree from source node s to destination nodes |d|, a tree is encoded by an integer routing table. Each row represents a routing path along the tree. Hence, when a tree T has route from s to D, the j-th row in the routing table will be $|R_t|$ and it list up the nodes IDs on the routing path from *s* to d_j along |T|. Therefore, R_t is routing table of |d| as shown in Fig 2. All the paths are encoded under the cost value and hop count.



Paths

s	1	3	d	Nul l	Nul l
s	1	2	4	d	Nul l
s	1	2	d	Nul l	Nul l
s	1	3	d	Nul l	Nul l
s	5	2	4	d	Nul l
s	6	7	d	d	Nul l

Fig. 2: Illustration of the path length solution

Population initialization: In the beginning, the population is filled with solutions that represent random paths. Even though the paths are random, they are supposed to be valid paths, where the solutions consist of a sequence of nodes that are in the path from source to destination. For example, source node s searches a random path to d by randomly selecting a node v_1 from N(s), the neighborhood of s. Then, randomly select a node v_2 from $N(v_1)$. This process is repeated until d is reached. Since, the path should be loop-free, those nodes that are already included in the current path are excluded from being selected as the next node to be added into the path, thereby avoiding reentry of the same node into a path. In this way, we get a random path P(s, d) = {s, v1, v2, . . . , d}. Repeating this process for q times, the initial population Q = {Ch0, Ch1, . . ., Chq -1} can be obtained. Hence, list of multiple valid paths will be generated. The length of path solution should not exceed the number of nodes in the network as shown in Fig 2. And the procedure of Electromagnetic-like Mechanism (EM) with Great deluge (GD) algorithm for routing protocol in MANET is illustrated in Fig 3.

Step 1: Initialization

Generate initial population (path_Soli);
Calculate the initial penalty cost for each solution(path), f(path_Soli);
Set best solution SolBest = path_Sol;
Update routing table.
Set initial level, Level = f(path_Sol);
Set total number of iterations, NumOfIte;
Set number of Iterations for Great Deluge, NumOfIte GD;
Set Iteration = 0

Step 2: Evaluation

do WhileIteration<NumOfIte)
Calculate total force, F, for each path based on EM;
Apply a dynamic force increment deluge algorithm;
Increase iteration by 1

end do

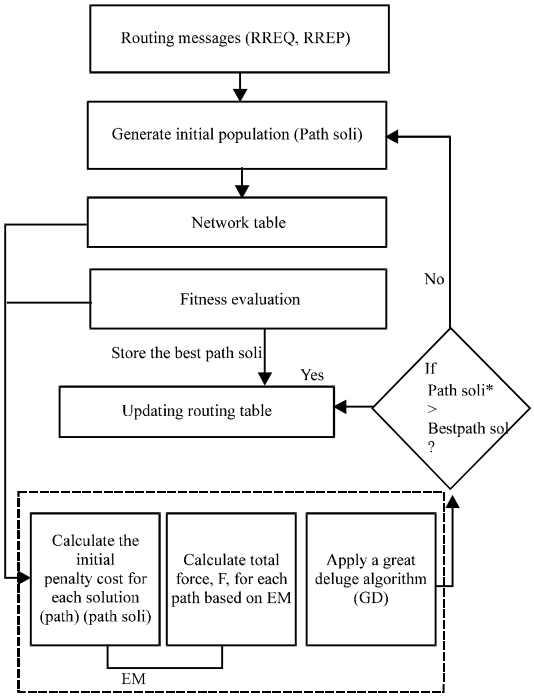


Fig 3: Electromagnetic-like Mechanism (EM) with Great Deluge (GD) Algorithm for Routing Protocol in MANET

Great Deluge (local search procedure)

Set number of iterations for Great Deluge, NumOfIte GD
Calculate estimated quality of every solution, EstimatedQuality = f(path_Soli) - Fi
Where i= 1 to population size;
Calculate force increment, ß = EstimatedQuality / NumOfite;
Set iteration GD = 0;
for (iteration GD<NumOfIte GD)
Select random node from path_soli and change it to a valid nodes to generate a new solution called path_Soli*
Calculate f(path_Soli*);
if (f(path_Soli*) > f(path_Solbest)) where path_Solbest represent the best solution found so far
path_Soli _ path_Soli*;
path_Solbest _ path_Soli*;
else
if (f(path_Soli*) > level)
path_Soli _ path_Soli*;
Increase iteration by 1;
end if
end if
level = level¡-β;
1. Increase iteration GD by 1;
end for

Simulation scenarios and parameters: In order to evaluate the efficacy and accuracy of the routing protocols, we performed a set of simulations based on ns-2 (Fall and Varadhan, 2003) with extensions for mobile wireless networks. This extended simulator has good support for simulating complete wireless network protocol model from physical and data link layer, MAC layer, routing layer to application layer. Lucent's WaveLAN (Anastasi *et al*., 2004; Tuch, 1993) is used as the radio model with 2 Mb sec^{-1} bit-rate and 250 m radio range. The MAC layer is implemented according to IEEE802.11 Distributed Coordination Function (DCF) (Anastasi *et al*., 2003). Each of the nodes began transmitting at randomly chosen location inside the simulation area. When the simulation started, the nodes remained stationary during a period of pause time (seconds). The nodes would then select random destination in the simulation area and moved towards that destination.

Some of the parameter that describes the characteristic behavior of an *ad-hoc* network is varied in a controlled manner. The parameters are:

- **Mobility:** Mobility is one of the most important characteristics of an *ad-hoc* network. This will affect the dynamic topology (links will go up and down)
- **Offered network load:** The load that we actually offer the network. This can be characterized by three parameters such as packet size, number of connections and the rate that we were sending the packets with
- **Network size:** (number of nodes, the size of the area that the nodes are moving within). The network size basically determines the connectivity. Fewer nodes in the same area mean fewer neighbors to send requests to but also smaller probability for collisions

In this evaluation, five performance metrics; packet delivery fraction, average end-to-end delay, normalized routing load, routing overhead and throughput are used to examine the robustness of our proposed algorithm. Table 1 explains the acronyms for those performance metrics:

- Packet delivery fraction:

$$\text{pdf}(\%) = \left\lfloor \sum \text{recvs} / \sum \text{sends} \right\rfloor \times 100 \tag{12}$$

Table 1: Acronyms for performance metrics

Parameters	Description
pdf	Packet delivery fraction
E2E	Average end-to-end delay
NRL	Normalized routing load
OH	Routing overhead
AHC	Average hop count
recvs	The packets successfully received
sends	The packets generated
PkTduration	The packets generated duration
recvnum	The number of packets received
RPgenThe routing packets generated RPrecvs	The routing packets received

- Average end-to-end delay of data packets:

$$E2E = \sum \text{packet duration} \Big/ \sum_{recv} \tag{13}$$

- Normalized routing load:

$$NRL = \sum RPgen \Big/ \sum_{RP recvs} \tag{14}$$

- Routing overhead:

$$RO = \sum RPgen \Big/ \sum_{RP sends} \tag{15}$$

- Throughput (KPPS):

$$\text{Throughput} = \left[\frac{\sum recv}{PKT duration} \right] \times (8/1000) \tag{16}$$

The first two matrices are important to justify the best efforts traffic while the routing load metric evaluates the efficiency of the routing protocol. These matrices were chosen because they are able to measure the efficiency of the routing protocol. It was expected that our trust mechanism could give higher packet delivery fraction with longer delay time and higher normalized routing load based on selecting the trusted path. If any errors prompt, fine tuning should be conducted to correct identified error.

Nodes misbehaviors: In this simulation, the trust values t and battery energy e values are assigned randomly with the condition that $t \in \{0 \geq t \leq 100\}$ for each node. Thus, the nodes may have different trust values. Therefore, nodes may have different trust value. The possibility of packet drops caused by node misbehaviors corresponds to the trust value t_v given to that node. The probability of each node to drop a packet, pd, is given by the following equations:

$$Pd(t) = 100\text{-trust value} \tag{17}$$

Simulation scenarios: In this simulation, two different scenarios were simulated. In the first scenario, 50 nodes are fairly distributed within 1500×300 m area with transmission range of 250 m. The pause time is fixed at 0 second and the simulation period is 900 sec. Nodes are allowed to move with range of 25 to 200 m sec^{-1} maximum speed and it is the essential parameter that is varied in this scenario. The parameters for scenario one is as shown in Table 2.

Figure 4 shows the comparison among EMNet, AntNet and AODV routing protocols in terms of packet delivery fraction. In this scenario, when the speed of node is low, the packet delivery fraction should be high for all three protocols due to the low mobility of the nodes in the network area. Thus, it will eventually lead to a stable network. However, as the speed of node increases, the percentage of packet delivery fraction for all three protocols will be decreases. EMNet performed

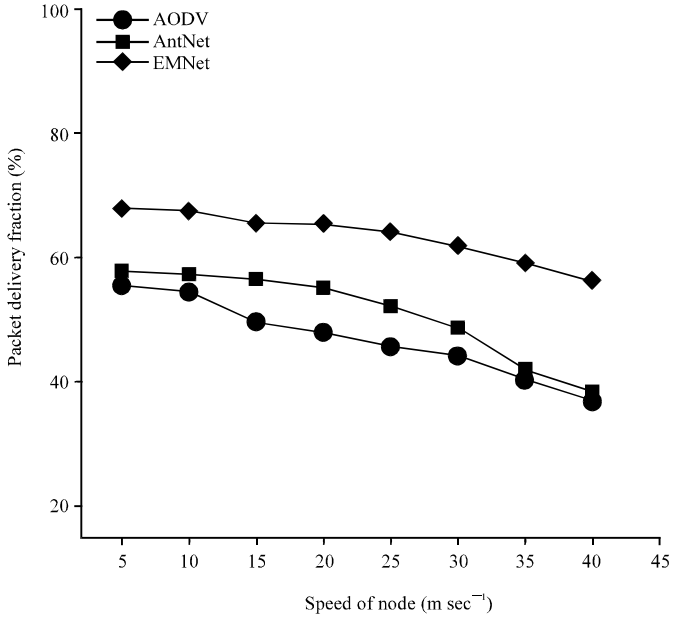


Fig. 4: Packet delivery fraction for scenario 1

Table 2: Simulation parameters for scenario 1

Parameters	Values
No. of nodes	50
Simulation time (sec)	900
Network area size (m)	1500×300
Max Speed of node (m sec^{-1})	25 to 200
Mobility model	Random way point
Traffic type	Constant bit rate (CBR)
Packet size (bytes)	512
Connection rate (pkts sec^{-1})	4
Pause time (sec)	0
No. of connection	5

particularly well while AODV and AntNet have very low percentage of packet delivery fraction during node misbehavior. The reason for AODV and AntNet to have higher percentage of packet drop is due to the broken link caused by misbehavior nodes. In EMNet, there is lesser broken link due to its multipath set from source to the destination.

The average end-to-end delay for EMNet, AntNet and AODV routing protocol is as shown in Fig. 5. Since the pause time equal to 0 sec (continuous motion) with varied movement speed, there will be broken routes due to unstable network. This will require the nodes to find a new route to the destination, which in turn will increase the end-to-end delay. However, EMNET has the lowest end-to-end delay compared to AntNet and AODV routing protocol. This is because theoretically, EMNet will allow sources to have a backup route to the destinations based on the route selection mechanism. Thus, EMNet only select route through trusted nodes with highest battery energy with acceptable number of hop count.

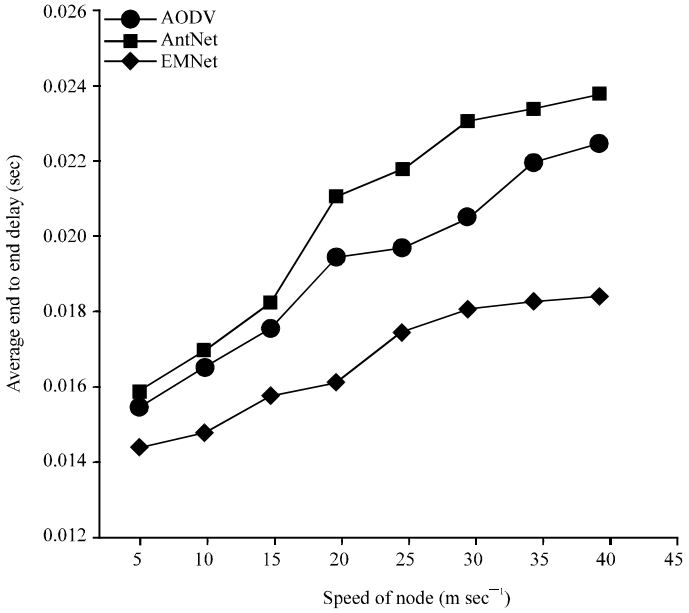


Fig. 5: Average end to end delay for scenario 1

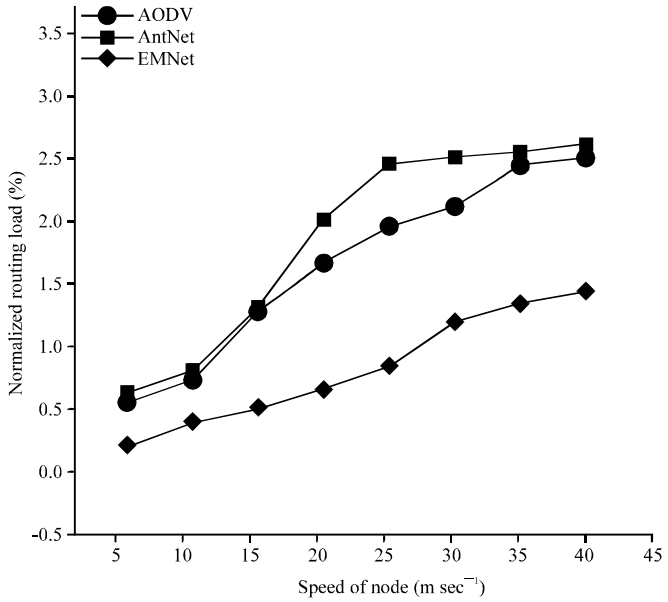


Fig. 6: Normalized routing load for scenario 1

Figure 6 illustrates the normalized routing load for EMNet, AntNet and AODV routing protocols. Theoretically, it will be expected that the normalized routing load in AODV and AntNet will increase due to the extra messages that need to be generated when the chosen path is no longer available due to the misbehaviour nodes and node in continuous motion with high speed. Hence, Nodes need to generate request messages in order to find new path replace the broken one. These messages will lead to high normalized routing load. However, the experiment result shows that EMMet has lower load compared to AODV and AntNet. The reason is, EMNet does not have

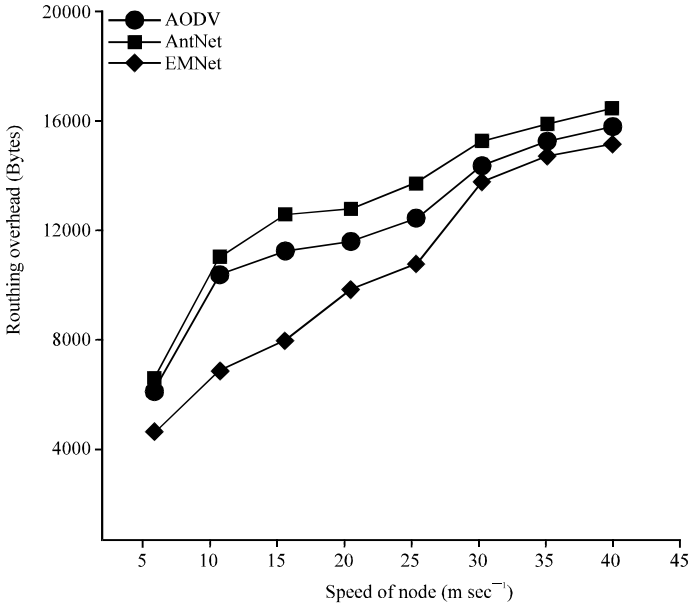


Fig. 7: Routing overhead for scenario1

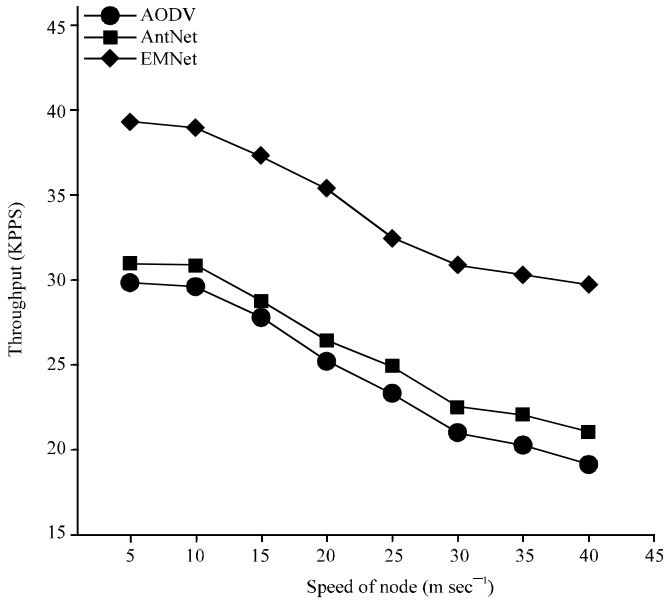


Fig. 8: Throughput for scenario 1

to do extra work to find a new route since the backup route is existing. However, EMNet performs better in term of normalized routing load by not having to recalculate its path so often.

The experimental result of the routing overhead shows that EMNet generates lower overhead compared to AODV and AntNet, as illustrated in Fig. 7. In AODV and AntNet, the rate for broken route is higher due to misbehavior nodes and therefore the nodes have to do extra work to find a new route. However, EMNet performs better by not having to recalculate its path frequently.

When the node movement speed is low, all three protocols give a high percentage of throughput, as shown in Fig. 8. However, as the node movement speed increases, the throughput of the

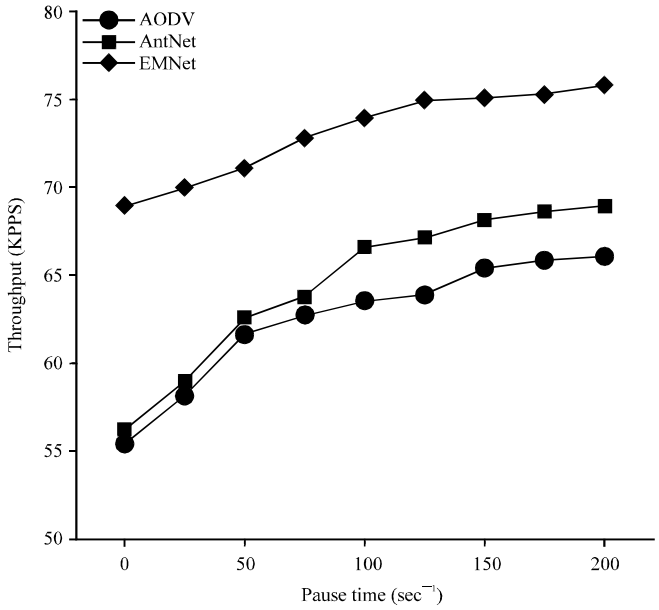


Fig. 9: Packet Delivery Fraction for scenario 2

Table 3: Simulation parameters for scenario 2

Parameters	Values
Number of nodes	50 nodes
Simulation time (sec)	900
Network area size (m)	1500×300
Max Speed of node (m sec^{-1})	25
Mobility model	Random way point traffic
Type	Constant bit rate (CBR)
Packet size (bytes)	512
Connection rate (pkts sec^{-1})	4
Pause time (sec)	0,25,50,75,100,125
Number of connection	5

protocols decreases due to changes in the topology of network which is caused by misbehavior nodes and high movement speed of node. However, EMNet is still able to provide higher throughput compared to AODV and AntNet due to the path selection mechanism and its multipath design.

In the sec scenario, the same parameter applies except that the pause time is now varied from 0 to 125 sec. Nodes are allowed to move up to the speed of 25 m sec^{-1}, which is a reasonable maximum speed. The parameters for scenario two are shown in Table 3.

The packet delivery fraction for EMNet, AntNet and AODV routing protocols for scenario 2 is shown in Fig. 9. In this scenario, EMNet has a better packet delivery fraction percentage when compared to AODV and AntNet for each set of connections. One of the reasons is EMNet generally selects route based on EM rules which depends on three different QoS (trust value, battery power and less hop count). Furthermore, EMNet can find alternate route if the current link has broken whereas AODV and AntNet are rendered useless at that point. Nevertheless, EMNeT shows good result in terms of packet delivery fraction compared to AODV and AntNet.

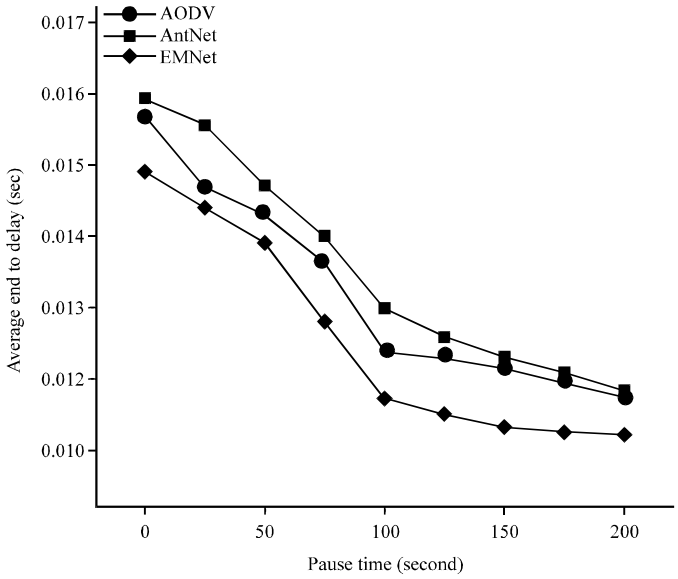


Fig. 10: Average end-to-end delay for scenario 2

Figure 10 illustrates the average end-to-end delay for EMNet, AntNet and AODV routing protocols. Since there are several misbehaved nodes in the network, there will be broken routes in the three test cases. In AODV and AntNet, the nodes are required to find a new route to the destination, which in turn increases the end-to-end delay while in EMNet have already pick up the route to the destination. Therefore, EMNet shows a better performance in term of end to end delay compared to AODV and AntNet.

Figure 11 illustrates the comparison among EMNet, AntNet and AODV routing protocols in terms of normalized routing load. For all the three test cases, normalized routing load reduces as the pause time increases due to the stability of network. However, EMNet has a better packet delivery fraction percentage compared to AODV and AntNet for each set of connections. AODV and AntNet may have much routing messages because sources nodes may have routes break to destination. In this case, nodes need to send request message to notify other nodes about that routes break. Hence, nodes have to discover new routes by sending other request messages. The broken routes are mainly caused by node misbehaviour or lacking of QoS. The characteristics of EMNet eventually helps to reduce routes break caused by misbehave nodes. This is because EMNet will select route based on three QoS requirements (trust, power and shortest). Thus, EMNet showed better performance in term of normalized routing load compared to AODV and AntNet.

According to Fig. 12, AODV and AntNet have higher percentage of routing overhead for any range of pause time. This is attributed to the different mechanism of AODV and AntNet compare to EMNet. As AODV and AnTnet belongs to the unipath routing protocol, the packet delivery along that route discontinue once the link is broken. In this case, they need to broadcast a new request looking for another route to the destination. However,

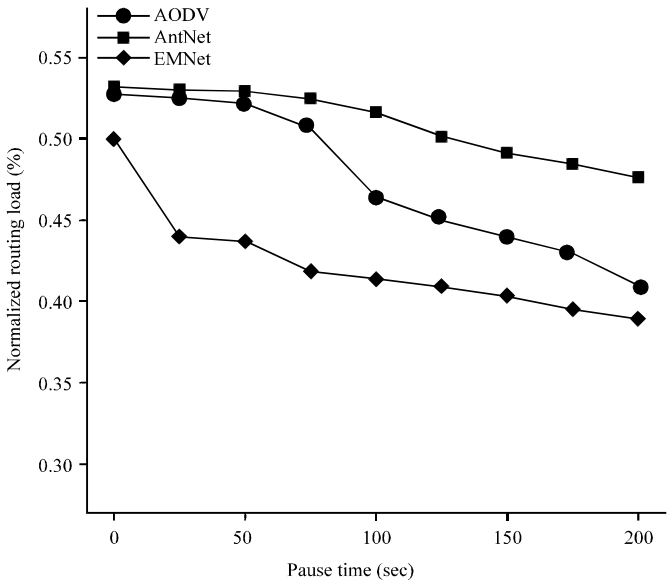


Fig. 11: Normalized routing load for scenario 2

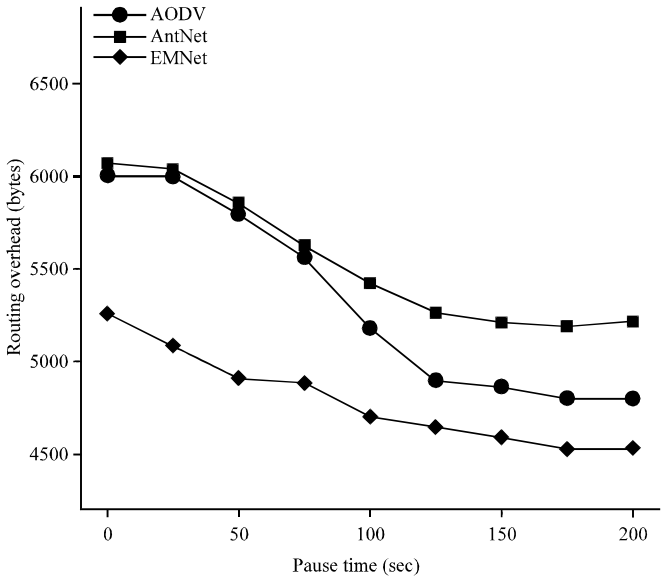


Fig. 12: Routing overhead for scenario 2

since EMNet is a multipath routing protocol, it has the ability to re-route using its backup path to the destination. Hence, AODV and AntNet incurs more routing overhead compared to EMNet.

As shown in Fig. 13, when there is no pause time (continuous motion), all the three test cases have a low throughput due to unstable network. However, as the pause time increases, EMNet shows better performance in term of throughput compared to

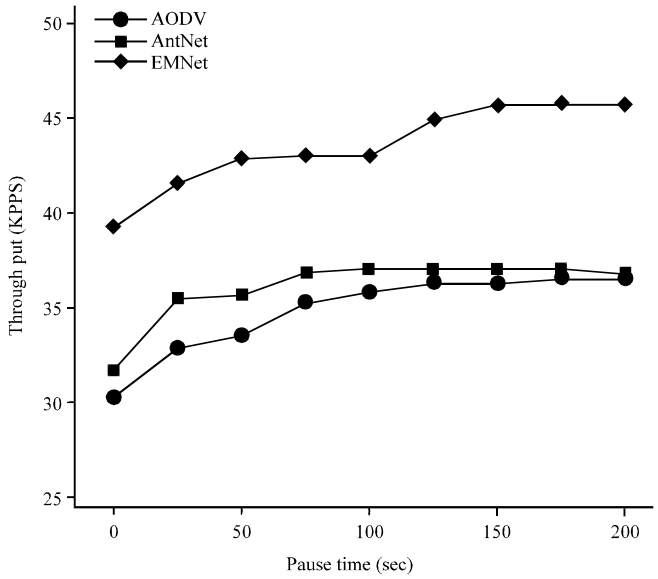


Fig. 13: Throughput for scenario 2

AODV, A ntNet for each set of connections. The reason is that EMNet will have backup routes for each destination when the current path is no longer available due to the high mobility.

CONCLUSION

The QoS problem is one of the major issues in routing protocols and is very difficult to be solved in MANET network due to its dynamic topology. Several research works have been done on dynamic unicast problem using the artificial intelligent technique to solve the QoS issues. However, none of the researcher has studied on incorporating Electromagnetic-like Mechanism (EM) in MANETs routing protocol. This study proposed a new approach of routing protocol using Electromagnetic-like Mechanism (EM) that is able to improve the QoS of dynamic uncicast in MANETs. Several network performance parameters have been selected for performance evaluation. Based on the simulation results, the proposed EMNet algorithm shows better routing performance in the simulated scenarios.

ACKNOWLEDGMENT

This work was supported by MOSTI (Ministry of Science, Technology and Innovation, Malaysia) with project code 01-02-03-SF0202.

REFERENCES

Anastasi, G., E. Borgia, M. Conti and E. Gregori, 2003. IEEE 802.11 *ad hoc* networks: Performance measurements. Proceedings of the 23rd International Conference on Distributed Computing Systems Workshops, May 19-22, 2003, Providence, RI., USA., pp: 758-763.

Anastasi,G.,M.Conti and E . Gregori, 2004.IEEE802.11AdHocNetworks:ProtocolsPerformance and Open Issues. In: *Ad hoc* Networking, Basagni, S., M. Conti, S. Giordano and I. Stojmenovic (Eds.). John Wiley and Sons Inc., New York, USA., ISBN-13: 9780471373131, pp: 69-116.

Birbil, S.I. and S.C.Fang, 2003.An Electromagnetism-like mechanism for global optimization.J. Global Optimiz., 25: 263-282.

Bonabeau, E., Dorigo, M. and G. Theraulaz, 1999. Swarm Intelligence: From Natural to Artificial Systems. Oxford University Press, New York, ISBN-13: 9780195131598, Pages: 307.

Broch, J., D.A. Maltz, D.B. Johnson, Y.C. Hu and J. Jetcheva, 1998. A performance comparison of multi-hop wireless *ad hoc* network routing protocols. Proceedings of the 4th Annual ACM/IEEE International Conference on Mobile Computing and Networking, October 25-30, 1998, Dallas, Texas, USA., pp: 85-97.

Buruhanudeen, S., Othman, M. and B.M Ali, 2007. Existing MANET routing protocols and metrics used towards the efficiency and reliability: An overview. Proceedings of the Telecommunications and Malaysia International Conference on Communications, May 14-17, 2007, Penang, Malaysia, pp: 231-236.

Cheng, H. and S. Yang, 2010. Genetic algorithms with immigrants schemes for dynamic multicast problems in mobile *ad hoc* networks. J. Eng. Appli. Artif. Intell., 23: 806-819.

Chuanhe, H., C. Yong, S. Wenming and Z. Hao, 2007. A trusted routing protocol for wireless mobile *ad hoc* networks. Proceedings of the IET Conference on Wireless, Mobile and Sensor Networks, December 12-14, 2007, Shanghai, China, pp: 406-409.

Fall, K. and K. Varadhan, 2003. Ns notes and documentation. Technical Report, The VINT Project, UC-Berkeley and LBNL.

Ghalavand, G., A. Dana, A. Ghalavand and M. Rezahosieni, 2010. Reliable routing algorithm based on fuzzy logic for mobile *ad hoc* network. Proceedings of the 3rd International Conference on Advanced Computer Theory and Engineering, August 20-22, 2010, Chengdu, pp: V5-606-V5-609.

Jassim, H.S., S. Yussof, T.S. Kiong, S.P. Koh and R. Ismail, 2009. A routing protocol based on trusted and shortest path selection for mobile *ad hoc* network. Proceedings of the 9th Malaysia International Conference on Communication, December 15-17, 2009, Kuala Lumpur, Malaysia, pp: 547-554.

Jing, F., R.S. Bhuvaneswaran, Y. Katayama and N. Takahashi, 2006. On-demand multipath routing protocol with preferential path selection probabilities for MANET. Proceedings of the 20th International Conference on Advanced Information Networking and Applications, Volume 2, April 18-20, 2006, Washington, DC., USA., pp: 758-762.

Johnson, D., Y. Hu and D. Maltz, 2007. The dynamic source routing protocol (DSR) for mobile *ad hoc* networks. IPv4, rfc4728.

Khan, K.U.R., R.U. Zaman and A.V. Reddy, 2008. Performance comparison of on-demand and table driven *ad hoc* routing protocols using NCTUns. Proceedings of the 10th International Conference on Computer Modeling and Simulation, April 1-3, 2008, Cambridge, UK., pp: 336-341.

Li, X., M.R. Lyu and J. Liu, 2004. A trust model based routing protocol for secure *ad hoc* networks. Proceedings of the IEEE Conference on Aerospace, Volume 2, March 6-13, 2004, Big Sky, Montana, USA., pp: 1286-1295.

Milanovic, N. and M. Malek, 2004. Routing and security in mobile *ad hoc* networks. Computer, 37: 61-65.

Perkins, C.E. and E.M. Royer, 2003. *ad hoc* on-demand distance vector (AODV) routing. IEFT Network Working Group, RFC 3561.

Rajabhushanam, C. and A. Kathirvel, 2011. Survey of wireless MANET application in battlefield operations. Int. J. Adv. Comput. Sci. Appli., 2: 50-58.

Rajagopalan, S. and C.C. Shen, 2006. ANSI: A swarm intelligence-based unicast routing protocol for hybrid *ad hoc* networks. J. Syst. Archit., 52: 485-504.

Tuch, B., 1993. Development of wave LAN, an ism band wireless LAN. AT and T Tech, pp: 27-33.

Woo, K., C. Yu, H.Y. Youn and B. Lee, 2001. Non-blocking, localized routing algorithm for balanced energy consumption in mobile *ad hoc* networks. Proceedings of 9th International Symposium on Modeling, Analysis and Simulation of Computer and Telecommunication Systems, August 15-18, 2001, Cincinnati, OH., USA., pp: 117-124.

Xie, F., L. Du, Y. Bai and L. Chen, 2007. Energy aware reliable routing protocol for mobile *ad hoc* networks. Proceedings of the Conference on Wireless Communications and Networking, March 11-15, 2007, Kowloon, Hong Kong, pp: 4313-4317.

Zeng, Y.Y. and Y.X. He, 2005. Ant routing algorithm for mobile *ad-hoc* networks based on adaptive improvement. Proceedings of the International Conference on Wireless Communications, Networking and Mobile Computing, Volume 2, September 23-26, 2005, Wuhan Univ., China, pp: 678-681.