Middle-East Journal of Scientific Research 23 (8): 1839-1850, 2015
ISSN 1990-9233

DOI: 10.5829/idosi.mejsr.2015.23.08.22491

Routing Optimization Security in Vanets using Adaptive Bees Life Algorithm for QoS-MRp and Batch Binding Update Scheme

[1]*K.R. Jothi and* [2]*A. Ebenezer Jeyakumar*

[1]CSE, Sri Ramakrishna Institute of Technology, Coimbatore, India
[2]Director-Academics, Sri Ramakrishna Engineering College, Coimbatore, India

Abstract: In view to provide continuous services for passengers, mobility management plays a major role in Vehicular Ad hoc Networks (VANETs). As Network Mobility (NEMO) is known for its high mobility, it becomes extremely suitable for VANETs. The vision for VANETs is road safety and aimed for efficiently dealing the mobility of a set of mobile nodes using Mobile Routers (MRs). However, inefficient routing paths, multiple tunnels and Quality of Service (QoS) requirements are major important issues of NEMO. In order to solve routing problem, proposed an novel Adaptive Bees Life Algorithm (ABLA) route optimization schema in NEMO and satisfies the QOS Multicast Routing Problem (QoS-MRP). The diversity of the space problem is estimated by using certain population characteristic values and the promising areas are exploited. Many of the traditional signatures security schemas in VANETs solve security problems for route optimization, but it leads to heavy computational costs. To overcome these issues, Batch Binding Update Scheme (BBUS) is proposed for secure accomplishment by verifying multiple signatures at the same time. The experimental results showed that the proposed algorithm is efficient in its performance in multicast traffic engineering and for evaluating the route stability in NEMO.

Key words: Mobility management . Vehicular Ad hoc Networks (VANETs) . Network Mobility (NEMO) . Mobile Routers (MRs) . Quality of Service (QoS) . QOS Multicast Routing Problem (QoS-MRP) . Batch Binding Update Scheme (BBUS) . multicast traffic engineering . route stability

INTRODUCTION

VANETS are able to simultaneously connect to different domains and radio access network technologies as each vehicle of it can have multiple radio interfaces [1]. Nowadays, there are limited vehicles to choose a default interface for sending and receiving informationinspite of those simultaneously connecting to these different network technologies simultaneously, nowadays vehicles are limited in choosing a default interface for sending and receiving information. This kind of limitation is related to the present model of multiple interface management in which several interfaces are attached to the operating system [2]. It is usual that the operating systems either use configuration files from the user or consider the application typesfor selecting a default network interface to send and receive data [3]. The information are acquired by the Vehicles through V2V (Vehicle to Vehicle) or I2V (Infrastructure to Vehicle) communications. The V2V communication is based on the Dedicated Short Range Communications (DSRC) technology whereas the V2I communication is based on GPRS/3G, WiFi or WiMAX. Mobility management plays a key role in VANETs for providing continuous services for passengers. The high mobility of vehicles make it difficult to maintain seamless handoff procedures and stable connections for Internet services [4]. It is again hard to maintain a seamless handoff and a stable connectivity to the Internet due to high moving speed of the vehicle in the VANET. Efficient assignment and reassignment of the IP of the mobile device can bring out seamless handoff for IP based communication. Johnson *et al*., [5] has proposed Mobile Internet Protocol version 4 (MIPv4) by means of the Internet Engineering Task Force (IETF). As MIPv4 has been facing problems such as short IP addresses and weak security mechanism, MIPv6 was proposed by IETF to alleviate the above problems [6].

An important characteristic of mobile IP can be configured by neighbour discovery or auto configuration. There are two types of auto-configuration mechanisms namely stateful and stateless mechanisms. Dynamic Host Configuration Protocol (DHCP) as adopted in both IPv4 and IPv6 is an example forstateful auto-configuration mechanism

Corresponding Author: K.R. Jothi, CSE, Sri Ramakrishna Institute of Technology, Coimbatore, India

[7] in which DHCP server manages and configures each IP address [8]. The stateless auto-configure mechanism is adopted by IPv6 by creating link-local IPv6 address. The MIPv6 is not much efficient as MIPv4 though it can provide enough IP addresses and better security mechanism compared to MIPv4. Hence, IETF has proposed a hierarchical mobile Internet Protocol (HMIPv6) in order to improve the efficiency of MIPv6 [9].

In HMIPv6, a new component named as Mobility Anchor Point (MAP) has been added for managing user's location. There are two types of location management in MAP such as the macro-mobility and micro-mobility managements among which the micro-mobility helps in improving the handoff efficiency of MIPv6. Both MIPv4 and MIPv6 are designed to handle terminal mobility however, not suitable for handling network mobility. The route discovery, maintenance and recovery are mainly focussed by the mobility management of V2V communications [9] while stable internet connectivity is taken care by V2I communications [10]. This paper attempts to improve both the security and efficiency of V2I mobility management. Therefore,MIPv6has been extended by the mobile working group at IETF to support Network Mobility (NEMO) [11]. The road safety and necessary comfort applications for vehicle drivers are been ensured by the principle VANETs. In this way, the vehicles act as communication nodes by offering data exchange to ensure the collision prevention and application of accident warning services as traffic information, breakdown and fuel services, office locations and so on.

In this paper, the study of multicast routing problem with quality of service (QoS-MRP) for VANETs is been performed as the combinatorial optimization belongs to the NP-Complete class. The finding of optimal tree called multicast tree from the source to the destinations (multicast group nodes) is the primary goal along with the achieving four objectives such as minimum cost, the reduced delay, the decreased jitter and the maximum bandwidth. Other than these, the expected tree should respect three QoS constraints with respect to transmission applications that are allowed for delay, jitter and a minimum bandwidth. This prolem can be solved by proposing a new Meta heuristic called Bees Life Algorithm (BLA). Among species colony optimization, BLA is a swarm intelligence algorithm and considered as asapproximate optimization method which performs based on the collaborative individual behaviours in the population. The lifecycle of the colony is closely imitated as it follows the two important behaviours of bees such as reproduction and the food foraging. As VANETs is known for its high mobility feature, a secure and efficient Batch Binding Update Scheme (BBUS) was proposed to simultaneously verify myriad of BUs in a correspondent node. In order to lessen the computational delay, Elliptic Curve Cryptography (ECC) is been further employed with ECQPVS in BBUS. Most of the security protocols especially NEMO BS focus only on the authenticity of the mobile node's BU for assuming the identity of true correspondent node. The remaining part of this paper is organized as follows: Section 2 presents a background of the used methods; Section 3 describes proposed ABLA with BBUS system. Section 4 gives the implementation results and analysis and finally Section 5 summarizes the conclusion remarks.

RELATED WORKS

Internet communication works on hierarchical IP addresses with a static (address) topology for routing IP packets between communicating peers. But in contrast, VANETs are highly mobile so that there is a dynamic change in VANET topology and moreover vehicles also permanently change their gateway to the Internet. The vehicles should be accessible from hosts in the Internet irrespective of their location. For instance, the applications for remote diagnostics are developed so that vehicle can be inspected through the Internet by a car vendor. Many schemes have been developed to study network mobility and thereby to improve the layer 3 handoff [12]. A handoff scheme to support network mobility over 802.16e was reported by [13]. The current study deals with both layer 2 and layer 3 handoff, however majorly for layer 3 handoff. A scheme called NEMO-SHO was proposed [14] as an advancement of the NEMO basic protocol so that it can be applied to the heterogeneous access network (Cellular networks and WLAN). A seamless vertical handoff can thus be achieved by equipping each mobile router (MR) with two interfaces.

A hybrid handoff scheme with multiple mobile routers called Intelligent Control Entity (ICE) was proposed by Lin *et al*. [15]. The multihoming for NEMO is being supported by this scheme and the handoff problem of the NEMO basic protocol is eliminated as an access router (AR) can manage number of access points (AP). The best AR is then chosen by the ICE for an MR. Both the intra-and inter-domain handoff are supported by ICE for providing a seamless handoff. The historical handover patterns of mobile devices are considered in a handover scheme with geographic mobility awareness (HGMA) [16]. The unnecessary handovers are prevented based on the received signal strength and moving speeds of mobile

devices. The method of handover candidate selection is also introduced in HGMA for mobile devices for selecting a subset of WiFi access points or WiMAX relay stations for scanning.

In case of PMIPv6, the design and implementation of flow mobility extensions was focussed to support dynamic IP flow mobility management across access wireless networks according to operator policies [17]. The feasibility of the proposed solution was assessed by considering energy consumption as a critical aspect for hand-held devices and smart-phones so that an experimental analysis showing the cost of simultaneous packet transmission/reception was provided using multiple network interfaces. The network is considered as the decision control entity in such work.

In order to maintain the Internet connectivity of vehicles, in [17] the author presented a PMIPv6-based NEMO (P-NEMO) which makes no participate in the management of location update when the vehicles are moving. An extension protocol of P-NEMO is a fast P-NEMO (FP-NEMO) which was developed to improve handover performance. The wireless L2 events are utilized by FP-NEMO so that to presume the handovers of vehicle. The preparation of vehicle handover is done before the vehicle get attached to the new access network by the mobility service provisioning entities. SEND protocol is a 128-bit IPv6 address which consists of a 64-bit subnet prefix and a 64-bit interface identifier [18]. Cryptographically Generated Address (CGA) is the 64-bit interface identifier which is computed by a cryptographic one-way hash function from the MN's public key and auxiliary parameters. A simple extension of the CGA is a Multi-key Cryptographically Generated Address (MCGA) [19] which further takes advantage of generation of MR's public key.

For solvingQoS-MRP, [20] applied Particle Swarm Optimization (PSO). Based on the computation result of PSO, the QoS requirements in many multimedia applications has been satisfied and an appropriate proxy core node was found in order to reduce control overhead [21].

In this work, a priority scheduler is also incorporated. Based on the packet delivery ratio, end-to-end delay and the overhead, the proposed approach has been compared successfully with ODMRP, DCMP and MPSP protocols. The extension of this study is performed by taking other important parameters such as the cost, jitter and bandwidth into account.A modified quantum-behaved PSO method for QoS multicast routing in MANETs was proposed by Sun *et al*. in [20]. Integration of this method with PSO and GA is then tested on random generated network topologies and hence superiority is demonstrated. However, the obtained results are based on non-strict constraints. An important optimization technique is artificial neural network (ANN) which has been investigated [22] to deal with the constrained multicast routing optimization problem in a mobile network. A reliable multicast route (tree) is computed by this approach and during a change in location of group members,a reliable route is selected due to mobility. Simulation results demonstrated the computational time performance of this method especially in the node mobility case. QoS based multicast routing problem resolution was brought on Tabu search algorithm [23] which considers two important QoS constraints such as the bandwidth and end-to-end delay. In addition to all these, the evaluation function was also determined by minimum cost of the multicast tree.

PROPOSED METHODOLOGY

The proposed study deals with the two main contributions. Firstly, the multicast routing problem is solved using quality of service (QoS-MRP) using Adaptive Bee Life Algorithm (ABLA) in Network Mobility. Secondly, a secure and efficient Batch Binding Update Scheme (BBUS) was proposed by taking high mobility feature of VANETs into account for simultaneous verification of myriad of Bus in a correspondent node. The computational delay is lessened by further employing Elliptic Curve Menezes-Qu-Pintsov-Vanstone Signature (ECQPVS) in BBUS. However, increase of the encrypted message size significantly more than RSA encryption is one of the main disadvantages of Elliptic Curve Cryptography (ECC). The implementation of ECC algorithm is more complex and difficult than RSA which further increases the likelihood of implementation errors thus to reduce the security of the algorithm. To overcome this problem, the proposed work implemented ECQPVS as the key agreement protocol and the proposed block diagram is represented as follows in Fig. 1.

Problem definition: The representation of VANET isby a weighted graph G = (V,E) where V denotes the set of nodes and E denotes the set of links connecting these nodes. Each set of link can be measured by four QoS items such as cost, delay, jitter and bandwidth. All these constraints were represented by the link transmission cost, the real delay during the link transmission, the real link transmission delay variation (jitter) and the estimated link bandwidth respectively. For any link ($e \in E$), some QoS metrics are defined

delay function: $Delay(e): E \rightarrow R^+$, cost function: $Cost(e): E \rightarrow R^+$, jitter function: $Jitter(e): E \rightarrow R^+$ and bandwidth function: $Bandwidth(e): E \rightarrow R^+$

The above problem is subjected to the following Qos

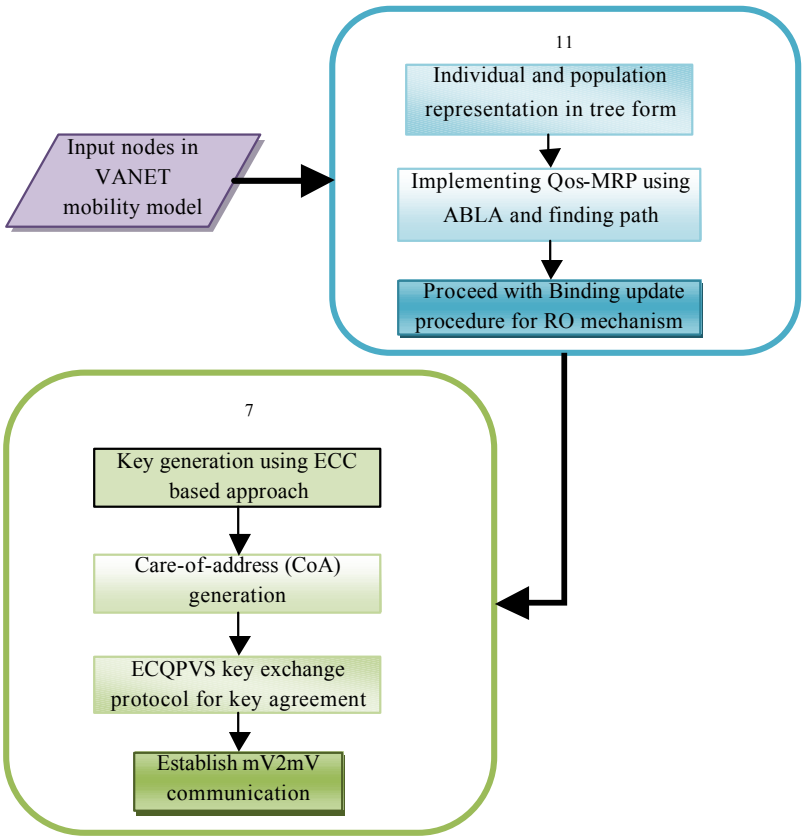

Fig. 1: Block diagram for proposed work

constraints:

Delay constraint: Delay (p(s,T))≤Q_D,

Jitter constraint: Jitter (p(s,T))Q_D

Bandwidth constraint: Bandwidth (p(s,T))≥Q_B

So, the minimization problem was represented by the quality of service multicast routing problem with constraints, where their fitness function is to find a multicast tree T(s,M) so that to minimize the weighted combination like cost, delay, jitter and bandwidth after satisfying the above mentioned constraints. Thus the problem is formulated as follows:

$$Min\ f(T(s,M)) = w_1 f_c + w_2 f_d + w_3 f_j + w_4 f_b \quad (1)$$

where

$$f_c = Cost\left(T(s,M)\right) \quad (2)$$

$$f_d = Max\left\{\sum_{t \in T} Delay\ (p(s,t))\right\} < Q_D \quad (3)$$

$$f_j = Max\left\{\sum_{t \in T} jitter\ (p(s,t))\right\} < Q_J \quad (4)$$

$$f_b = \underset{t \subset T}{Min}\left\{\sum_{t \in T} Bandwidth\ (p(s,t))\right\} < Q_B \quad (5)$$

Here, w_1, w_2, w_3&w_4 are the objective weighting coefficients used for evaluating the problem relating to the importance of these four objectives.

Bee life algorithm: Bees life algorithm operates as a resemblance of bee population in which an initialization step contains N bees (individuals) that are chosen at a random in the search space. The second step follows the evaluation of population fitness. A bee population constitutes one queen, D drones and W workers in which the fittest bee represents the queen, the D fittest following bees represent the drones and the remaining bees are the workers. As a consequence, the sum of the different bee individuals (1,D & W)is equal to the population size (N). DandW are considered as a two user defined parameters. Every lifecycle of bee population consists of two behaviours related to bee such as reproduction and food foraging. The initiation of reproduction behaviours in the space is by means of mating-fight between the queen and the drones using crossover and mutation operators.

The breeding of the queen gives rise to N broods followed by which the evaluation of the brood fitness is performed. The fittest is considered as the new queen after which it the next brood is fitter than the queen, it will be population. Moreover, D fittest is taken as the following broods and the current population is formed by the drones of the next population. Then, W best bee individual is searched among the W fittest remaining broods and the foraging of food is done by workers of the current population. The W workers search food source in W regions of flowers by considering that each worker represents one region. There are also other bees for each region which are recruited and employed to search the best food source among the population. The evaluation of the new population fitness is then executed. A new bee life cycle is performed until the stopping criterion is not satisfied followed by which the third step is rerun and so on. The step by step algorithm of BLA is given below

STEP 1: Initialize population (N bees) at random

STEP 2: Evaluate fitness of population (fittest bee is the queen, D fittest following bees are drones, W fittest remaining bees are workers)

STEP 3: While stopping criteria are not satisfied (Forming new population)/* reproduction behavior*/

STEP 4: Generate N broods by crossover and mutation

STEP 5: Evaluate fitness of broods

STEP 6: If the fittest brood is fitter than the queen then replace the queen for the next generation

STEP 7: Choose D best bees among D fittest following broods and drones of current population (Forming next generation drones)

STEP 8: Choose W best bees among W fittest remaining broods and workers of current population (to ensure food foraging)/* food foraging behavior*/

STEP 9: Search of food source in W regions by W workers

STEP 10: Recruit bees for each region for neighborhood search (more bees for the best B regions)

STEP 11: Select the fittest bee from each region

STEP 12: Evaluate fitness of population (fittest bee is the queen, D fittest following bees are drones, W fittest remaining bees are workers)

STEP 13: End while

ABLA for QoS-MRP and RO: The application of ABLA to the QoS-MRP and route optimization is presented in this section. First, the individual and population representations are introduced. Second, ABLA initialization and fitness function are initiated and explained to evaluate the individual and/or the population. The various operators such as the crossover, the mutation and the neighborhood searching used in ABLA are also explained. Next, the iterations stopping criterion and final a complexity analysis of ABLA are explained. Here the adaptive strategy rapidly increases the exploitation of good solutions so that speeding up of the population can be converged and prevented from getting stuck in most cases. The pseudo code for ABLA is given in the flowchart as shown in Fig. 7.

Pseudo code for Adaptive Bee Life Algorithm

1. **Initialize population (N)**
2. **Evaluate Fitness (Q,D,W)**
3. **While (i<MaxIT)**
4. **Do reproduction (D)**
5. **Adaptive Selection p_c(N), P_m(N)**
6. **Evaluate fitness (broods) by using**

$$\text{Min } f(T(s,M)) = w_1 f_a + w_2 f_d + w_3 f_j + w_4 f_b$$

7. **If fit_brood>Q**
8. **Cycle=cycle+1**
9. **Choose best one (D)** /* reproduction behavior */
10. **Else**
11. **Choose best one (W)** /* food foraging behavior */
12. **End if**
13. **neighborhood Search food_source(W)**
14. **Recuirt best_bees(W)**
15. **Fittest bee(D,W)**
16. **i=i+1**
17. **Until i = MinIT**
18. **End while**

IndividualandPopulationRepresentation: The first step in the algorithm is represented in this phase. In the proposed network, the individual is represented as single solution which is multicast tree containing the different paths from source node to each multicast group members (destinations) through a set of intermediate nodes. With the help of a string expressed by order on node path numbers, path is encoded [24]. The representation of an individual is by tree structure containing its different paths. The example having the rear twenty (20) vehicles or mobile (nodes) in the VANET is given in Fig. 2. The nodes are represented by circles and their links which is shown with the helpof a line between two nodes.

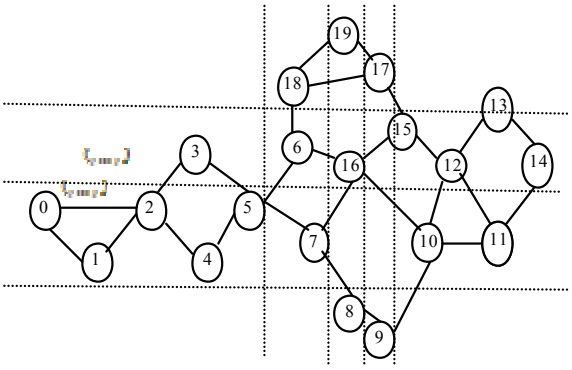

Fig. 2: Explanatory and theoretical VANET

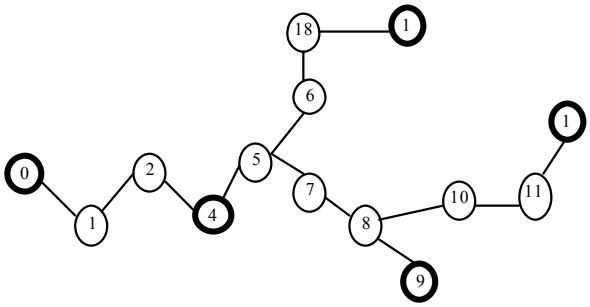

Fig. 3: An example having the rear twenty (20) vehicles (nodes) in the VANET

For example, if there is link between node 0 and node1 with link cost=220, delay=124 ms, jitter=1.8 ms and bandwidth=797.54kbit/s. The cost is the function of the link distance measured in meter which is reconsidered equally in the experimentation. If a source node s is considered as node 0 and the multicast group members (destination nodes) are nodes={4,9,14,19}, then the individual can be chosen as the tree shown in Fig. 3. This tree contains four paths each one is string of nodes, from the source s (node:0) to one of each destination (nodes:4,9,14,19). The four paths are: (0-1-2-4),(0-1-2-4-5-7-8-9),(0-1-2-4-5-7-8-10-11-14),(0-1-2-4-5-6-18-19). The populations iscollection of a set of individuals where their number is a user parameter.

Initialization and reproduction: VANETs could be represented by its different topology data such as nodes number, their locations and their different links. Besides, between two adjacent nodes, cost, delay, jitter and bandwidth are used to specify each link. The search space of the QoS-MRP problem is also defined from whichN individuals (solutions) are randomly generated to construct the initial population. Each individual is represented by tree which contains M paths from source node to M destinations. Note that M is the number of multicast group and the source node is the root of the tree representing the individual. The weighted aggregation (WA) method is applied to evaluate the individual [25].

Incase of QoS-MRP Problem, an intuitive way of obtaining Multiobjective optimization is carried out especially when only one solution should be obtained. This is more adequate in this context than Pare to approach. In the WA approach, different objectives are weighted and summed up to a single objective and taken as the fitness function [26]. The population fitness is the sum of the individual's fitness. In the reproduction part of the ABLA, two major operators such as crossover and mutation are applied. The neighbourhood search approach is executed in case of foraging part. In this subsection, the application of generating new individuals is been explained.

Crossover: It is a binary operator in which the queen is selected and one drone is randomly chosen to generate two new individuals. This process is repeated until reaching N individuals with crossover probability of p_c. We propose the following crossover operator for this tree representation as two-point crossover. For both parents, two paths for two destinations of the population is in by observing the two objective characteristics namely fitness value of the best member f_{max} and average fitness $\overline{f}$ of the set of solution both assigned to current generation. The resulting value of $f_{max} - \overline{f}$ is likely to be less for population that has converged than for a population scattered in the solution space. However, without proper scaling mechanism this can be vary significantly from case to case, because adjusting the values of fitness to have similar relations regardless of the problem under consideration.

To avoid this problem the normalized expression is used in determining the degree of population diversity: $f_{max} - \overline{f} / f_{max}$. In this to exploit the degree of population diversity the correlation technique is performed in each generation. If the new value is greater than the old one, the value of the variable is then replaced with new one. If it is lower, the adaptive mechanism takes effect. The choice of the solutions to be crossed is done by calculating their indexes in the following manner; $i = N.r^{exp}$. where N is the population size, i is the index of the member to participate in crossover and r a randomly generated number between 0 and 1. The best number is assigned number 1 and worst N. If exp equal to 1, the chromosomes are picked uniformly; if exp is greater than 1, index i is lower and 'better' solutions are favored. The parameter exp is evaluated as follows:

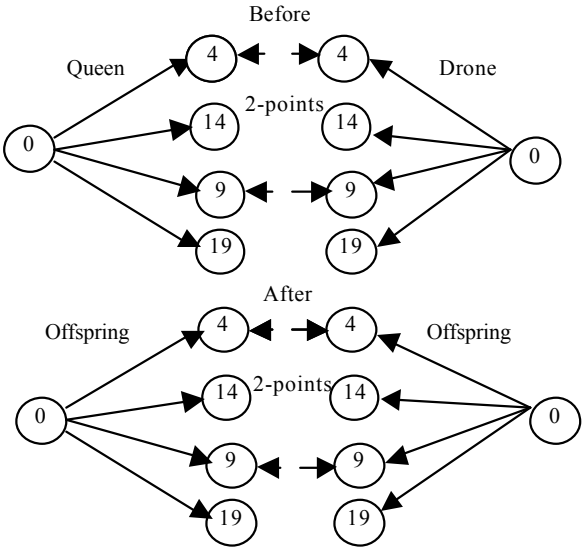

Fig. 4: Cross-over operator

$$exp = k_1 + k_2 \cdot \left(\frac{p}{corr}\right)^2$$

where p is the current generation and corr for the value stored in the static variable. Before calculating exp the algorithm compares the p andcorr and replaces the corr with new value if p>corr. In this algorithm the values assigned for k_1&k_2 is assigned as $k_1 = 0.0$ and $k_2 = 3.0$. The result will be replaced by the towpaths towards the same destinations for the second parent and vice versa. The crossover is illustrated in Fig. 4.

MUTATION

The offspring are contingently to be mutated through the mutation probability of p_m which makes mutation a unitary operation process. The author recommends the following mutation operator. An offspring to be mutated has to follow two paths towards two destinations randomly chosen are selected. By adaptive strategy a node was selected for the same intermediate node which was selected already for the former node. Thus the mutation is getting adapted with different way the method only varies the number of mutations to be done. Numb er of mutations n is calculated as follows:

$$n = k_3 \cdot N \cdot \frac{(corr - p)}{corr}$$

where N is population size. The constant k_3 assigned value of 2.0.

If p is lower than corr, which corresponds to a more homogeneous population, the number of mutations

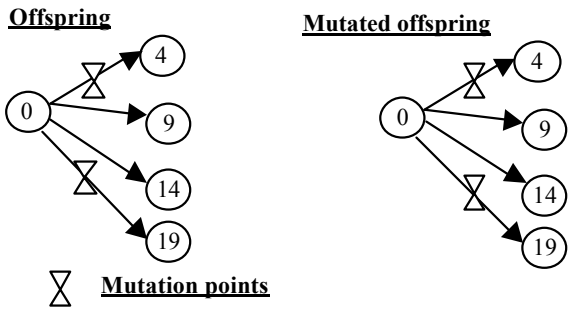

Fig. 5: Mutation operator

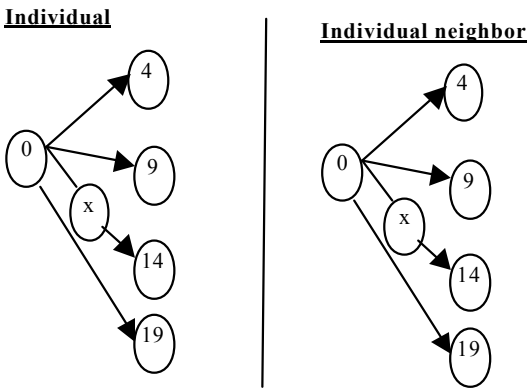

Fig. 6: Neighborhood search approach

increases linearly. If the same node is being initiated in the second paths (mutation2-points), the second part of the second path is joined to the first part of the first path and vice versa.If the chosen intermediate node is not found, this process is repeated until success. This function is illustrated in Fig. 5.

Neighborhood search approach: Neighborhood search in the foraging part of ABLA helps in reaching the neighbor individual from the original individual. The proposedapproach is a greedy approach by generating neighbor individual. In this approach, one individual path is randomly chosen and replaced by another path towards the same destination as the first one. It should contain at least one common intermediate node. Neighborhood search approach is illustrated in Fig. 6.

Stopping criterion: A dynamic stopping criterion can be fixed as a threshold. The ABLA iterations are carried out and stopped only when the population fitness won't change.MinIT times; it is the stagnation state. We note that the iterationsnumber is constrained by a maximum threshold MaxIT of iterations. The user parameters of this approach arenumbers MinIT and MaxIT.

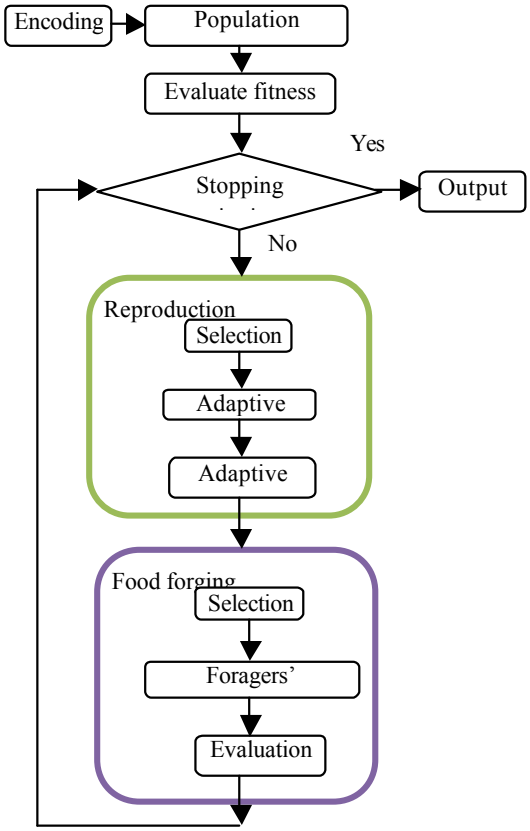

Fig. 7: Flowchart for adaptive bee life algorithm for RO

Secure and efficient batch binding update scheme: In this section, a secure route optimization scheme was followed in mobile IPv6 environment which was introduced as some security requirement. In the proposed scheme, we take the example of Mobile Nodes (MNs) that directly execute the Route Optimization (RO) tasks with its CNs. Simultaneous verification of binding updated messages forms the main contribution of the this scheme. Even if the RO tasks are performed by the Mobile Router (MR) instead of the MN, the merit of our scheme exists as well. The Multi-key Cryptographically Generated Address (MCGA) [20], a simple extension of the CGA, is used to ensure the address ownership of MN.

Key generation: First, we conjecture that the HAs of MNs are authoritative to issue the pair of signing/verification keys for MNs, with the public keys of HAs known by CNs. According to MIPv6, a MN and it's HA will share a pre-established security association to build a secure tunnel by IPsec ESP. The pairs of signing / verification keys to MNs were conveyed through the IPsec tunnels by the HA having the advantage over it. The Home Agent (HA) sets the following parameters: Let G_1 be a cyclic additive group generated by the generator P and G_2 be a cyclic multiplicative group. Both G_1 and G_2 have the same order q. Let e: $G_1 \times G_1 \rightarrow G_2$ be a bilinear map with the following properties

(1) bi-linearity: for all $P,Q \in G_1$ and $a,b \in Z_p^*, e(aP,bQ) = e(P,Q)^{ab}$;
(2) non-degeneracy: There exists $e(P,Q) \neq 1_{G_2}$;
(3) computability: there is an efficient algorithm to compute e(P,Q).

The HA picks a random numbers $s \in Z_p^*$ as the private key and generates the public key $PK_{HA} = sP$. Each MN_i possesses a pair of the signing key $SignK_i = s \cdot H(r_i \| ID_i)$ and the corresponding verification key $VerK_i = H(r_i \| ID_i)$, where $\|$ is a concatenation operation and KD(·) is a key derivation function, $r_i \in Z_p^*$, as well as ID_i is the identity of MN_i. When MN was moving from its home network into a foreign network the pair of signing/verification keys can be delivered by the HA. In addition, how many pairs of signing/verification keys are to be loaded can be decided by the expired time of keys.

Care-of-address (CoA) generation: When a MN_i moves into a foreign network, the Mobile Router (MR) belonging to the foreign network will send a Mobile Network Prefix (MNP) as router advertisement message. Then the MN_i signs the CoA_i by its signing key $SignK_i$, to generate the signatures, which is stored in a Neighbor Solicitation (NS) message. According to [20], the ownership of the CoA_i only delegated by the MN_i since nodes cannot produce the valid signatures of the MN_i and MR. The formula of the message signing is shown as follows:

$$\sigma_{MN_i} = h(msg_i \| T_i) \cdot SignK_i$$

where msg_i is denoted the content of the delivered messages and T_i the current timestamp to withstand replay attacks.

Binding update procedure for RO mechanism: After receiving the CoA_i, MN_i performs the following binding update procedure. Figure 8 illustrates the signaling and data flows of the proposed binding update procedure. In the first step, the Binding Update request BUReq message $\{N_i, HoA_p, CoA_i, x_iP, VerK_i, T_i, \sigma_{MN_i}\}$ where N_i the fresh random nonce and x_iP is a parameters of Elliptic Curve Menezes-Qu-Pintsov-Vanstone Signature (ECQPVS) key exchange protocol and Message Recovery type algorithm, is sent from MN

to its CN. This protocol provides many advantages for both computational and storage aspects. After receiving the message, the CN first verified the validity of timestamp T_i and signature σ_{MN_i} via the verification key $VerK_i$. Note that a popular CN may receive multiple BUReq messages in a short period, so the CN may wait a short period to simultaneously verify a number of binding update messages. For ease of presentation, we first introduce the single BUReq verification and then the details of the batch BUReq verification are also presented. ECQPVS is authenticated, so it does not suffer Man in the Middle (MitM) attacks. Key Derivation Function (KDF) Single and Batch BUReq verification: Given the system public parameters $\{G_1,G_2,q,P,PK_{HA}\}$ and the BUReq message $\{N_i, HoAp,CoA_i, xP, VerK_i, T_i, \sigma_{MN_i}\}$ sent from the MN_i, the

$$e(\sigma_{MN_i}, P) - e(KDF(mgs_i||T_i) \cdot VerK_i, PK_{HA})$$

which is verified as follows:

$$e(\sigma_{MN_i}, P) = e(h(mgs_i||T_i) \cdot SignK_i, P)) \quad (6)$$

$$= e(h(mgs_i||T_i) \cdot sKD(r_i||ID_i), P) \quad (7)$$

$$= e(h(mgs_i||T_i) \cdot KD(r_i||ID_i), sP) \quad (8)$$

$$= e(h(mgs_i||T_i) \cdot), VerK_i, PK_{HA}) \quad (9)$$

For the Given multiple n BUReq messages $\{N_i, HoAp,CoA_i, xP, VerK_i, T_i, \sigma_{MN_i}\}$ sent from the MN_j and the system public parameters, the CN can verify these multiple n BUReq messages where j = 1 to n.

If the result of the signature verification is positive; the Correspondent Node (CN) believes that the BUReq messages are sent from the communicating MNs. Then, in order to prepare the BURep1 message for MN_i's HA, the CN picks a fresh random nonce N_{CN} as an index for MN_i and the parameters like yP of the ECQPVS key exchange and message recovery protocol was being generated. Note that the CN only generates an ECQPVS parameter yP and delivers to multiple MNs involved in this batch verification. Because the values of $\{N_{CN}, N_i, yP\}$ will be forwarded to the MN_i. The CN employs the keyed key derivation function to generate the message authentication code

$$KDMAC_{CN} = h_{K_{BU_i}}(N_{CN}, N_i, yP)$$

where

$$K_{BU_i} = y(x_iP) = yx_iP$$

Note that the use of keyed key derivation function as the message authentication code of the value $\{N_{CN}, N_i, yP\}$ can speed up the message verification performed in MN_i. To ensure the integrity of BURep1 messages, the CN produces a signature σ_{CN} and delivers the BURep1 message $\{N_{CN}, N_i, yP, KDMAC_{CN}, HoA_i, CoA_i, T_{CN}, Cert_{Cn}, \sigma_{CN}\}$ to them MN_i's HA.

While receiving the BURep1 message from the CN, the MN_i's HA first verified the validity of timestamp T_{CN} and signature σ_{CN} and then checks whether the received HoA_i and CoA_i also can be found in its binding cache. If yes, the HA extracts the values of $\{N_{CN}, N_i, yP, KDMAC_{CN}\}$ as the BURep2message and forwards them to the MN_i via the pre-established IPSec tunnel; otherwise, this session is dropped. After obtaining the BURep2 message, MN_i first computes the binding key

$$K_{BU_i} = y(x_iP) = yx_iP$$

to check the validity of both $KDMAC_{CN}$ and its chosen nonce N_i. If the $KDMAC_{CN}$ is legal, MN_i can realize that the fresh nonce N_{CN} and the ECQPVS parameter yP are sent by the CN. Then the MN_i directly sends the BUMsg $\{CN, HoA_i, CoA_i, KDMAC_i\}$ to the CN for the purpose of the key confirmation. The BUMsg includes the CN's address CN, the MN's HA HoA_i, the care-of-address CoA_i and the message authentication code

$$KDMAC_i = h_{K_{BU_i}}(N_i, N_{CN}, CN, HoA_i, CoA_i$$

Note that the fresh nonces N_i and N_{CN} are implanted in the message authentication code against replay attacks. Once getting the BUMsg $\{CN, HoA_i, CoA_i, KDMAC_i\}$, the CN first extracts the nonces N_i and N_{CN} and then examines the validity of $KDMAC_i$. If both verifications succeed, the CN also checks whether the values of CN, HoA_i, CoA_i are the same as ones in BUReq. If all of them are the same, the CN can assure that the claimed HoA_i and CoA_i are believable. In the end, both the MN_i and CN update

$$K'_{BU} = h(K_{BU}, N_i + 1, N_{CN} + 1)$$

as the new binding update key in a subsequent session.

EXPERIMENTAL RESULTS AND DISCUSSION

When one node focuses to get the optimal multicast tree, BLA was executed instantly. For this specific reason second 85 has been chosen as an instant of

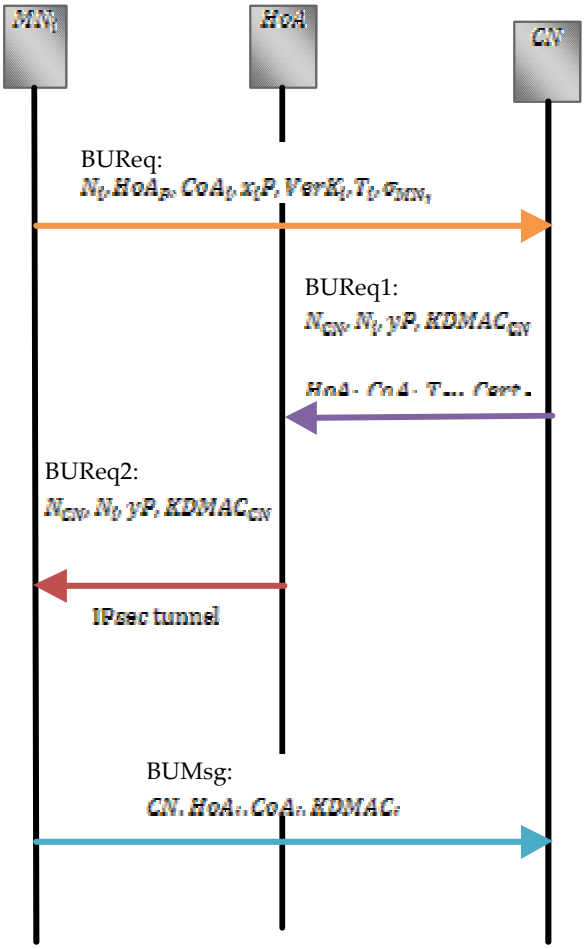

Fig. 8: The proposed binding update procedure for RO mechanism

experimentation. They are extracted from simulation scenario execution. Trace file generated by NS2 was used to extract the four metrics values of links between each two nodes. By the methods of IPSec and signature, our scheme provides a resistance to man-in-the-middle attack. By the technique of batch verification and elliptic curve cryptography,our scheme can mitigate the damage of Denial-of-Service (DoS) problems. Thus the performance of the proposed scheme with the other related works in terms of computational and communication costs were compared.

Fitness vs generation: Figure 9 shows the best multicast trees reached by BLA and ABLA respectively. To demonstrate the performance of ABLA in terms of computation time for fitness is compared to BLA the average rounded values of ten (10) best fitness obtained in each test for different algorithms are calculated. This figure elucidates the stagnation of the best solution fitness by each algorithm for each population with time consumed. BLA algorithm

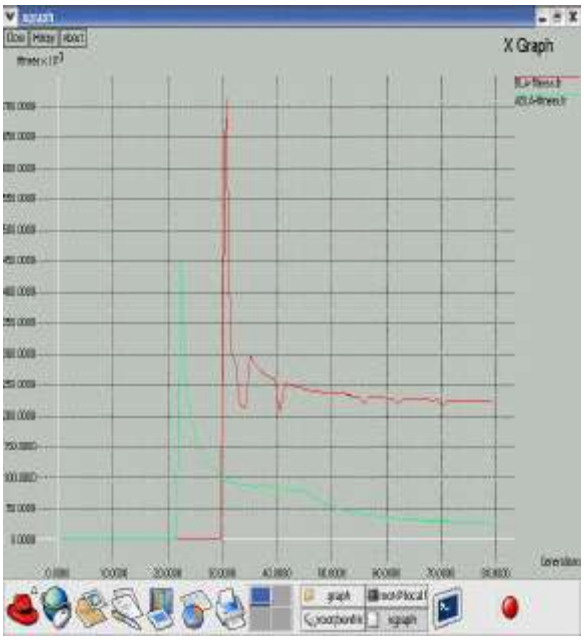

Fig. 9: Best solution fitness in generations (iteration times)

reaches the best fitness (26,969.80) in the BLA generation (12th generation). This proves its low time complexity compared to the others approaches. This practical analysis showed that ABLA converge to the optimal solution better than BLA with the least generation times. They confirm the reliability and efficiency of BLA to solve the QoS-MRP with a minimum time compared to other approaches.

Computational and communication cost: Considering multiple n binding update messages, the total computational costs are evaluatedfor those schemes with lightweight computational costs like MIPv6, caTBUA usually accompany with more messages to transmit. The BBUS's computational cost is computed as follows:

$$n \times (2T_{mul} + 2T_{sig ECQPVS}) + (1T_{mul} + +1T_{ver ECQPVS}) \approx 8.2n + 2.55ms$$

and illustrated in Fig. 10

For best results, we have evaluated the relationship of computational costs and binding update messages. Moreover, we further discuss the computational cost in Fig. 10. As you can see, our proposed scheme outperforms BBUS with ECDH when the number of binding update messages is more than 2. Thus for a fair view some schemes do not support the same security properties as ours, so we do not take their schemes into comparison. Figure 11 demonstrates the relationship

Fig. 10: Computational cost comp arison

Fig. 11: Communication cost comparison

between communication costs and binding update messages. When a large Communication costs (ms) number of binding update messages come, the communication costs of BBUS can be significantly decreased.

CONCLUSION

The quality of service multicast routing problem for vehicular ad hoc networks has been studied in this paper as multi-objective optimization problem with constraints. The objectives are to overcome the drawbacks such as transmission cost, delay, jitter and bandwidth. a novel algorithm inspired by the bee life called Adaptive Bees Life Algorithm is also prroposed. In order to prove the reliability and the efficiency of this proposal, a VANET simulation in NEMO model has been carried out according to the routing protocol that includes the implemented ABLA. Here a Batch Binding Update Scheme (BBUS) proposed with ECQPVS protocol to securely and efficiently accomplish route optimization procedures. ECQPVS is authenticated, so it does not suffer Man in the Middle (MitM) attacks. In fact, BBUS is designed for NEMO environment where a mobile router serves as the gateway to multiple mobile nodes. BBUS can verify a single binding update message if the waiting time for multiple binding updates messages is too long. From the experimental results, both the computational and communication costs are significantly reduced by using BBUS and ABLA conventional algorithms thus proving the efficiency and the performance of the proposed algorithm in terms of the solution quality and complexity for QoS-MRP problem.

REFERENCES

1. Blanchet, M. and P. Seite, 2011. Multiple interfaces and provisioning domains problem statement. IETF RFC 6418: 1-22.
2. Wasserman, M. and P. Seite, 2011. Current practices for multiple-interface hosts. IETF RFC, 6419: 1-21.
3. Makaya, C., S. Das and F. Lin, 2012. Seamless data offload and flow mobility in vehicular communications networks. IEEE in Wireless Communications and Networking Conference Workshops (WCNCW), pp: 338-343.
4. Al-Surmi, I., M. Othman and B.M. Ali, 2012. Mobility management for ip-based next generation mobile networks: Review, challenge and perspective. Journal of Network and Computer Applications, 35: 295-315.
5. Johnson, D., C. Perkins and J. Arkko, 2004. Mobility Support in IPv6, Internet Engineering Task Force (IETF), RFC-3775: 1-165.
6. Droms, R., H. Packard, B. Volz, T. Lemon, C. Perkins and M. Carney, 2003. Dynamic Host Configuration Protocol for IPv6 (DHCPv6), Internet Engineering Task Force (IETF), RFC-3315: 1-101.
7. Droms, R., 1997. Dynamic host configuration protocol, Internet Engineering Task Force (IETF), RFC, 2131: 1-45.

8. Soliman, H., C. Castelluccia, K.E. Malki and L. Bellier, 2005. Hierarchical Mobile IPv6 Mobility Management (HMIPv6), Internet Engineering Task Force (IETF), RFC, 4140: 1-29.
9. Papadopoulos, A., A. Navarra and J.A. McCann, 2011. Pinotti CM. Vibe: An energy efficient routing protocol for dense and mobile sensor networks. Journal of Network and Computer Applications, 35 (4): 1177-1190.
10. Zhu, K., D. Niyato, P. Wang, E. Hossain and D.I. Kim, 2011. Mobility and handoff management in vehicular networks: A survey, Wireless Communications and Mobile Computing, 11 (4): 459-476.
11. Devarapalli, V., R. Wakikawa, A. Petrescu and P. Thubert, 2005. Network Mobility (NEMO) Basic Support Protocol, Internet Engineering Task Force (IETF), RFC, 3963: 1-33.
12. Han, Y.H., J. Choi and S.H. Hwang, 2006. Reactive handover optimization in IPv6-based mobile networks. IEEE Journal Selected Areas in Communications (JSAC), 24 (9): 1758-1772.
13. Zhong, L., F. Liu, X. Wang and Y. Ji., 2007. Fast Handover Scheme for Supporting Network Mobility in IEEE 802.16e BWA System. IEEE International Conference on Wireless Communications, Networking and Mobile Computing (WiCOM), Shanghai China, pp: 1757-1760.
14. Naoe, H., M. Wetterwald and C. Bonnet, 2007. IPv6 Soft Handover Applied to Network Mobility over Heterogeneous Access Networks. IEEE International Conference on Personal, Indoor and Mobile Radio Communications (PIMRC), Athens, pp: 1-5.
15. Lin, H. and H. Labiod, 2007. Hybrid Handover Optimization for Multiple Mobile Routers-based Multihomed NEMO Networks. IEEE International Conference on Pervasive Services (ICPS), Turkey, pp: 136-144.
16. Yang, W.H., Y.C. Wang, Y.C. Tseng and B.S.P. Lin, 2010. Energy-efficient network selection with mobility pattern awareness in an integrated WiMAX and WiFinetwork. International Journal of Communication Systems, 23: 213-230.
17. Melia, T., C. Bernardos, A. de la Oliva, F. Giust and M. Calderon, 2011. Ip flow mobility in pmipv6 based networks: Solution design and experimental evaluation, Wireless Personal Communications, 61: 603-627.
18. Arkko, J., J. Kempf, B. Sommerfeld, B. Zill and P. Nikander, 2005. SEcureneighbor discovery (SEND, IETF RFC 3971: 1-56.
19. Jo, M. and H. Inamura, 2008. Secure route optimization for mobile network node using secure address proxying. In: IEEE/IFIP network operations and management symposium (NOMS), pp: 137-143.
20. Sun, J., W. Fang, X. Wu., Z. Xie and W. Xu, 2011. QoS multicast routing using a quantum-behaved particle swarm optimization algorithm, Engineering Applications of Artificial Intelligence, Elsevier, 24: 123-131.
21. Huang, C.J., Y.T. Chuang and K.W. Hua, 2009. sing particle swam optimization for QoS in ad hoc multicast. Engineering Applications of Artificial Intelligence, 22: 1188-1193.
22. Kumar, B.P.V. and P. Venkataram, 2003. Reliable multicast routing in mobile networks: A neural-network approach, Communications IEE Proceedings, 150: 377-384.
23. Forsati, R., A.T. Haghighat and M. Mahdavi, 2008. Harmony search based algorithms for bandwidth-delay-constrained least-cost, Computer Communications, 31: 2505-2519.
24. Bitam, S., M. Batouche and E.G. Talbi, 2010. A survey on bee colony algorithm, 24thIEEE International Parallel and Distributed Processing Symposium, NIDISC Work-shop, Atlanta, Georgia, USA, pp: 1-8.
25. Miettinen, K., 1999. Nonlinear Multi-objective Optimization, Kluwer.
26. Lee, J.H., T. Ernst and N. Chilamkurti, 2012. Performance Analysis of PMIPv6-Based Network MObility for IntelligentTransportation Systems, in IEEE Transactions on Vehicular Technology, 61: 74-85.