Circuits and Systems, 2016, 7, 1079-1086
Published Online May 2016 in SciRes. http://www.scirp.org/journal/cs
http://dx.doi.org/10.4236/cs.2016.77091

Scientific Research Publishing

Privacy Preserving Bee Routing Protocol for Intermittently Connected Mobile Networks

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

[1]Department of CSE, Anna University, Regional Campus, Madurai, India
[2]Department of CSE, Vaigai College of Engineering, Madurai, India
Email: itz_ramesh87@yahoo.com, pravvin.it@gmail.com

Received 24 March 2016; accepted 24 May 2016; published 27 May 2016

Abstract

The Intermittently Connected Mobile Networks (ICMN) is a disconnected mobile network where a complete connectivity never exists. More number of moving nodes makes them impenetrable genre which in turn makes the network intermittently connected. Detection of malicious node and routing is onerous due to its genre. In this paper, we put forward a secure routing that aids in detecting and preventing intrusion of malicious nodes. The routing process is made more adorable through Bee Colony Optimization (BCO). The amalgamation of BCO with authentication series leads a novel routing protocol named Privacy Preserving Bee Routing Protocol (PPBRP) which is highly secure. The degree of security is tested with malicious nodes in the network to prove that the proposed PPBRP ensures secure routing.

Keywords

Mobile Network, ICMN, PPBRP, BCO, Authentication Series

1. Introduction

Conventional network begins with wired communication which is long lasting which paves way to wireless communication. Network has its phase where communication takes place via sensor within the nodes popularly called as wireless sensor network. Another scheme where the network topology changes to time has a routing problem to be solved. Mobile Ad Hoc Network (MANET) runs through into existence where the topology and nodes keep changing. Recently, Intermittently Connected Mobile Networks (ICMN) [1] explore a new epic where due to high density, the connectivity is impossible leading to erratic territory.

Many routing protocols are derived to establish effective data communication Distance Vector Routing, Link State Routing (LSR), Open Shortest Path First (OSPF), Opportunistic Adaptive routing, Distance Source routing

How to cite this paper: Ramesh, S. and Praveen, R. (2016) Privacy Preserving Bee Routing Protocol for Intermittently Connected Mobile Networks. *Circuits and Systems*, **7**, 1079-1086. http://dx.doi.org/10.4236/cs.2016.77091

(DSR), Ad Hoc on demand Distance Vector (AODV) [2], Destination-Sequenced Distance Vector (DSDV) etc. But these protocols have not suit for ICMN.

ICMN is a network designed to operate effective over extreme distances. Mobility of nodes plays an important role in these delay tolerant networks (DTNs). Examples reflecting ICMN's are wild life tracking, habitat monitoring sensor networks, military networks, nomadic community networks, vehicular networks etc. Flooding, epidemic, direction based routing adaptive routing, utility based routing are some of the routing strategies proposed for ICMANET's. These routing strategies consider the effectiveness of data transmission but lack the focus on secure communication [3].

The goal in secure routing is to ensure safety against hostile nodes, which have an added advantage of preventing itself from unknown threats. Throughput of data routing like low delay, low memory capacity, varying bandwidth should not be eradicated in the process of creating authenticated routing. In this paper, we introduce a new methodology called Privacy Preserving Bee Routing Protocol (PPBRP) which focuses on maximum degree of security without any loss in the regular characteristics of data routing.

Here the network is parted into n divisions followed by source and sink selection. We go with a Bee Colony Optimization (BCO) strategy for data transmission preceded by neighbor challenge method which is nothing but the connected node details. Data transmission is initiated with neighbor node challenge and then proceeds with sharing the lists, identity tracking and code generation. The node is declared as an authenticated one only if it satisfies all those conditions which give way for data transmission. This is how the proposed technique promises for secure data communication.

This paper comprises of 3 more sections that describe the literature survey, proposed principle and corresponding result analysis respectively.

2. Related Work

Evolution of routing over years is been discussed in this section. Recent problem with the data communication in ICMN is added along with the literature survey. One of the trending networks is intermittently connected network where data packet routing is a tedious process. General summary of routing strategies applicable in this kind of network is bestowed here. Few routing protocols are explained below.

One of the traditional routing scheme for ICMANET is the flooding [4] based routing. In this approach, a particular node sends packet to all other nodes in the network where every node acts both as a transmitter as well as receiver. Each node tries to forward the message that it receives to other nodes that are its neighbours. Thus possibly every node receives the message that is circulated over the network. Flooding based technique paves the way as the basis for epidemic routing where periodic pair wise connectivity is necessary in message delivery. In this approach the message are dispatched immediately across the network [5]. Routing happens within the confined areas of the network which is based on the node mobility of carriers.

The single copy case routing [6] works on the principle that only one message copy forwarded to the target mode over the network whereas the multiple copy case routing [7] is based on disseminations of multiple copies of the message over the network. After the multiple copies are disseminated then the routing ensures that the packets reach the destined node. The spray and wait [8] is yet another technique which uses the spraying technique. The message or copy of the messages is sprayed and these messages are expected to get in contact with the target node. Until this phase the node is made to wait. This algorithm reduces the transmission overhead by holding a bound on number of copies and transmission per message.

The history of encounters and transitivity is focused in Probabilistic Routing protocol. Probabilistic term known as delivery predictability [9] for the destination is computed for each node, which is used to manipulate node's interest to transfer message. Facing nodes transfer the Summary vectors along with the delivery predictability data stored at the nodes, which in turn helps to update internal predictability is updated and the messages from other nodes are fetched via forwarding strategy. The semi probabilistic routing (SPR) [10] scheme works on the principle that the network is divides into partitions' that are stable in topology. If the destined node lies within the same topology it receives the forwarded data packets. If the node lies in some other topological zone the data packets are simple forwarded to the group that will guarantee the highest probability of delivery of the messages.

These routing techniques don't promise any data security. Since security is a salient feature in network communication to prevent data theft by hackers. To ensure that we introduce a new routing scheme called privacy

preserving bee routing protocol using BCO technique.

3. Privacy Preserving Bee Routing Protocol

The Privacy Preserving Bee Routing Protocol (PPBRP) is designed to ensure secure routing in ICMN. The initial network topology is split into n × n regions, where n is any positive integer. The network region is partitioned to entitle that the network is intermittent in nature. The network partition enables easy determination of destination and allows data transmission across it. The data transmission is possible with the help of the relay nodes. The region where the source region node resides is called the source region similarly region where destination node resides is the destination region [11]. The region enclosing the relay nodes aiding connection between the source and destination node is termed the candidate region. The node movement and the course of events are tracked down through the transition matrix.

The routing withholds certain parameters namely staying time, hitting time and return time. The destination region is selected based on the Time to Live (TTL) of the data packets that are transmitted. Based on the delivery delays, the selection for the candidate region is made. The delivery delay is the sum of the routing and the waiting time [12]. The choices of regions are made based on two criterions namely the frequency of visit by the destination node and the required time interval to reach the destination from the source node. The two criterions mentioned above are evaluated by routing time and waiting time respectively. Due to the mobile nature of the nodes, the datum are intended to be route through the relay nodes and is chosen based on the expected hit time.

Following the general setup for the routing protocol, the process of communication is described. The network region is partitioned into n × n regions. The source and destination regions are set as the packet to be transmitted is generated at the source node and the selection of destination node by source node is made respectively. Subsequent to this, the candidate region and the relay nodes are selected. The transmission of data packet between the nodes is done along with the authentication series. The routing is achieved with BCO. BCO [13] is used as it has the capability of delivering data packets frequently and with limited delay.

From **Figure 1**, BCO [14] routing initially the source node selects a relay node within its radio range and forwards the data packet towards it. The intermediate nodes that come within the radio range of the current relay node holding the data are chosen for next transmission. When delivering data to each node encountered, the objective value (OV) is incremented, which is initially set to 0. The OV is generally to estimate the efficiency of

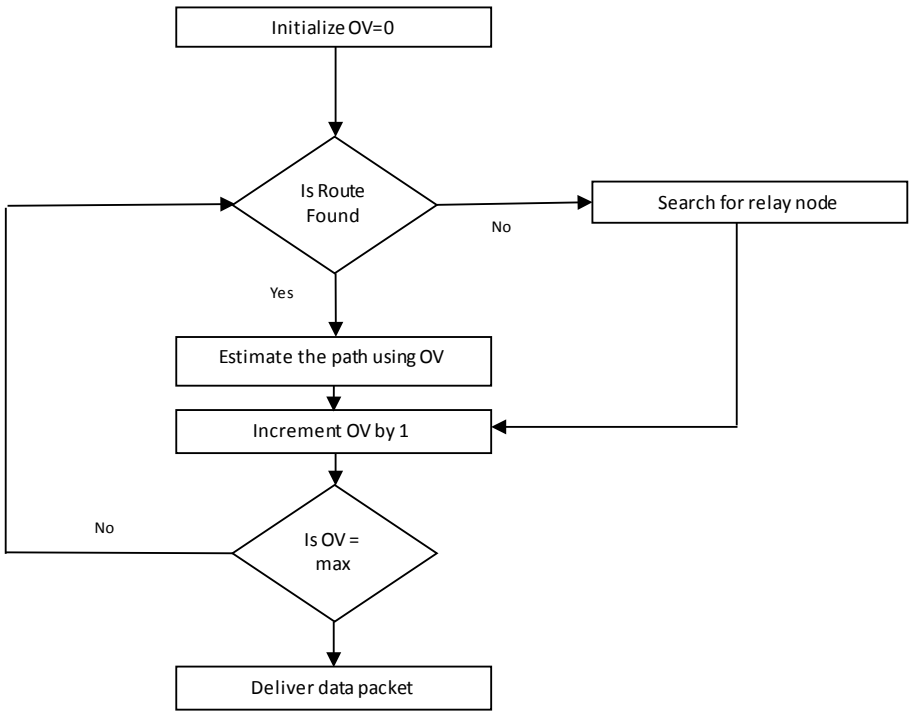

Figure 1. Working of PPBRP.

the path chosen for routing data packet. BCO has two phases namely forward phase and backward phase respectively. During forward phase the data is routed by selecting the intermediate nodes. The data packet traverses through the intermediate nodes from the source node and once it reaches the destination, the backward phase initiates. In the backward phase, the nodes share information about the path it has chosen. The OV on successful delivery of data towards destination increases. The path with maximum OV is assured to be the successful path to deliver the data [15].

During data transmission at each node encounter, the authentication [16] series is adopted. The initial step in the series is the identity tracking. The sender node requests for the IP address of the node it has currently encountered. The relay node replies the sender with its IP address. If the received IP address matches with the one in buffer maintained by sender, the relay node is assumed to be the trusted node. Each node maintains a trustee list, a list that contains details about the entire trusted node in the network and an untrustee list, a list that maintains information about all the malicious or suspicious nodes of the network. A buffer at each node holds the IP address of all the other nodes in the network, from its initial placement and also its public key.

A neighbor challenge is passed to estimate whether the primary relay node is a trusted node or a malicious node. It includes transmitting any of the pair of positive prime integers (a, b) available to it. The data is encrypted before forwarding it to the relay node. The neighbour challenge is forwarded through two possible routes, one holding the test node and the other is the known node. On receiving the challenge, secondary relay node computes cd mod n [17] and sends back the result to the sender through the two paths defined. The sender compares the result received from two paths. If both are same, the test node is assured to be a trusted node. The sender adds the test node to the trustee list, if the results differ sender appends it to the untrustee list. The challenge process is initiated only if the sender node doesn't find the relay node currently it has encountered in its trustee list.

As a sequence the trustee and untrustee lists are shared between the nodes, to have a history about all the trusted nodes in the network. During sharing process, the nodes compare the lists and they append the nodes that are found to be absent in it. The authentication series involves a pair code generation test. In this the sender node generates a random code and forwards it to the relay node in an encrypted form. If the relay node decrypts and sends back the same code, it is assured to be the trusted node. When these authentication series are passed by the encountered node, it is assured to be fully trusted and the data transmission is allowed. The BCO [18] along with authentication series enables PPBRP efficient. The receiving of ack adhere the complete transmission of data. The route with higher PHV is said to be the most attractive route and frequency of data transmission through that route is higher. PPBRP ensures secure data transmission in ICMN.

From **Figure 2**, it is evident that the algorithm for proposed PPBRP is depicted. Here the initial set up of OV is made then the process of bee movement to search the next intermediate node is specified with forward phase and the value of OV is analyzed with the backward phase.

4. Simulation Results

Simulation results of the proposed new technique of PPBRP. Epidemic routing and spray and wait routing pro-

```
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()
```

Figure 2. Pseudocode for PPBRP.

tocols are being compared with the proposed technique. Scenario set up for examining is described in Section 4.1 followed by influence of transmission range and the malicious nodes influence exhibition in Section 4.2.

4.1. Scenario Setup

The parameters set are the basic ONE (Opportunistic Networking Environment) Simulator [19] environ parameters and are given in **Table 1**. Mobility and the real time message passing could be viewed in its graphical user interface by a simulating environment called ONE which is also proficient to create node moments with varying movement patterns. Examining the routing protocols and DTN application is the prime feature of this simulator. In assistance with the synthetic movement model variety users are allowed to generate layouts and vestiges the real world followed by implementing routing and application protocols by provided framework. Experiences examining is aided by visualization tools and interactive post processing and the ONE simulator is a part of a real-world test bed DTN only if an emulation mode authorizes [20].

4.2. Influence on Transmission Range

Behaviour of routing protocols plays a vital role in transmission range. Changing the transmission range from 50 - 250 the three protocols ER SNW and PPBRP are examined. It demonstrates the coverage area of specific node to which data is to be transmitted. Performance of the proposed technique is examined by changing metrics latency, delivery ratio and overhead in varying transmission range. On doing so the protocols ER, SNW and PPBRP changes dynamically. Due to its pair-wise connectivity ER bestows higher ratio of overhead. Every node transfers the data packet to the first neighbouring node it meets which leads to high overhead. Since the data transfer takes place in wait phase, overhead in SNW is optimal. In the proposed technique the overhead is acceptable and little larger than SNW. In case of packet delivery PPBRP stands in front of ER and SNW which is showcased in **Figure 3**.

Generally ICMN comprises of extreme delays, so the routing protocols should be designed in a way to bear them. ER and SNW delivers a little late than PPBRP that makes the proposed scheme to be best. In SNW the node having single copy of packet waits so long despite of time while in ER pair-wise connectivity gives rise to delay. Due to region split up PPBRP reaches the destination node than ER and SNW. **Figure 4** depicts that the delay in ER and SNW is larger than PPBRP underlining PPBRP as a best among three.

ER has low delivery rate due to high chance in loss of data. This is because of nodes traversing in wrong path. In ER it has to wait too long which gives room for low delivery. In the proposed technique region selection is based on the data delivery rate. **Figure 5** is all about PPBRP's ability to deliver data 60% than ER and SNW.

4.3. Influence of Malicious Nodes

Number of hostile nodes eliminated from the network and number of data packets traversed via hostile node decides the standard of PPBRP. The capacity of secure routing scheme in identifying the hackers in the network is depicted by eliminated nodes in the network. **Figure 6** clearly displays the PPBRP's high capability to detect hostile node than ER and SNW. PPBRP uses authorization terms failing to which is marked as hostile node, while ER and SNW depend on intermediate nodes that reduce the probability to detect the hostile nodes. Since sharing process is used for authorization number of nodes is directly proportional to number of malicious nodes

Table 1. Basic simulation parameters.

Parameters	One Simulator
Area	2000 × 2000 m
Mobility Model	Random Waypoint
Node Density	50 nodes
Node Speed	1.5 m/s
Radio Range	250 m
Packet Life Time	600 s

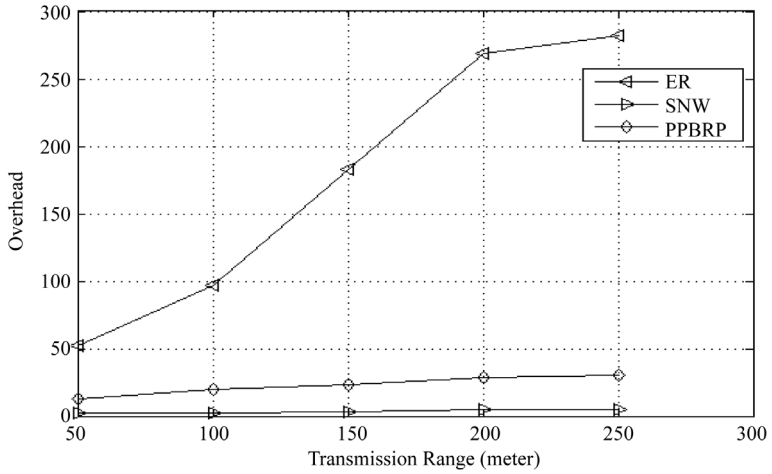

Figure 3. Overhead with respect to Transmission Range.

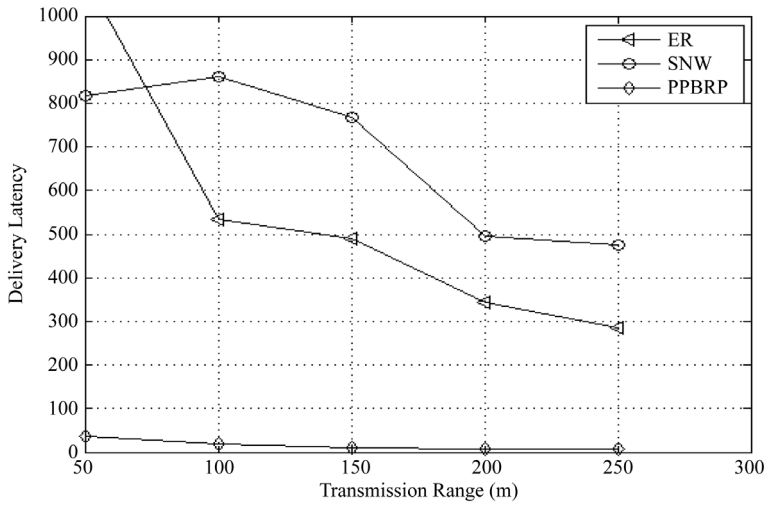

Figure 4. Delivery latency with respect to Transmission Range.

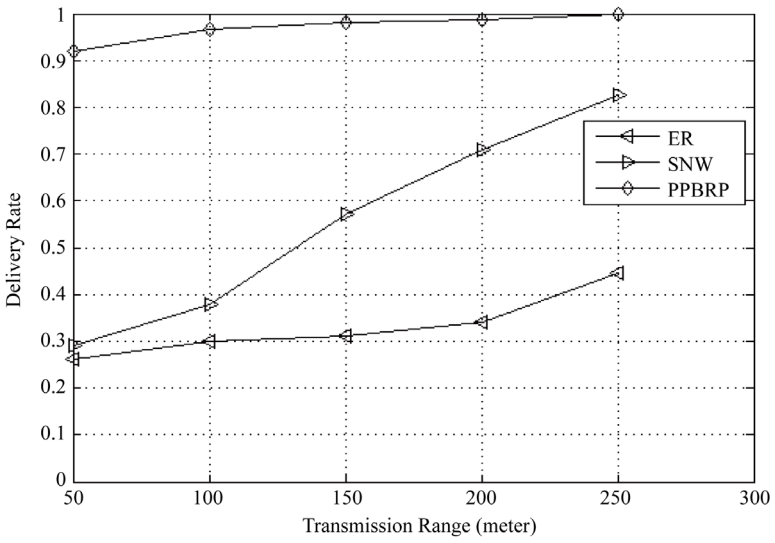

Figure 5. Delivery rate with respect to Transmission Range.

detection. In ER and SNW there is no such sharing schema which makes the detection a tough one. Probability of routing is less in PPBRP than ER and SNW when number of packets routed via hostile node is taken into account. **Figure 7** shows lesser transmission of packets via hostile node in PPBRP is because of potent identification of hostile node which is not present in ER and SNW. These terms clearly depicts that PPBRP is best for secure routing in ICMN.

5. Conclusion

Secure routing PPBRP is exhibited in this paper. This protocol provides a good standard of security in ICMN. Encompassing the security mechanism makes no change in the routing performance. Neighbour challenge gives way to integrity check within the network. It delivers data to the destination node without any deviation in the routing performance. In case of overhead, it shows 38% difference from SNW and 25% from ER while in delivery latency it is of 80% and 89%. It varies 88% and 72% respectively in case of delivery rate. Varying hostile

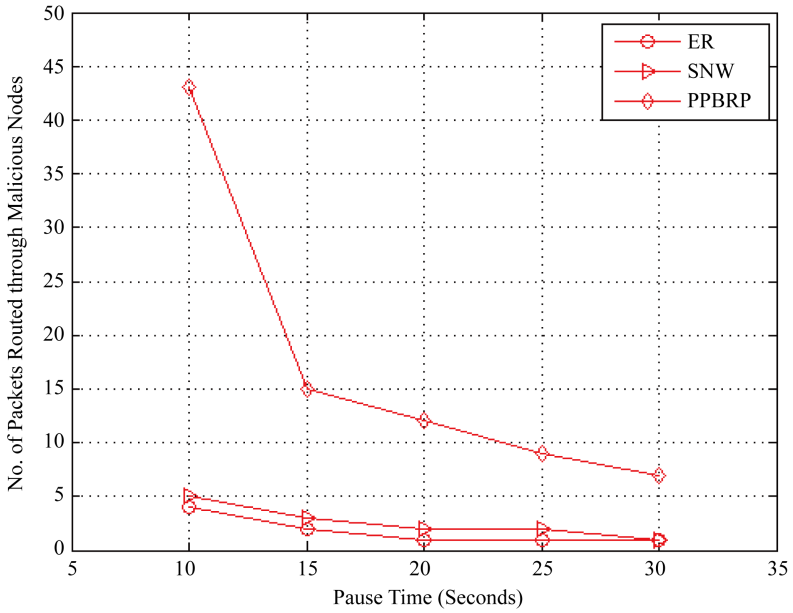

Figure 6. Number of malicious nodes isolated with respect to mobility.

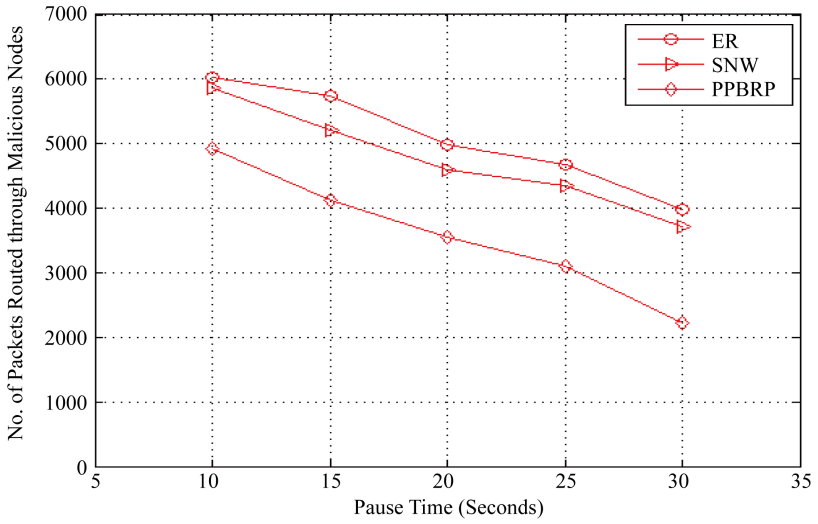

Figure 7. Number of packets routed through malicious nodes with respect to mobility.

node in assistance with mobility and number of nodes manifests the level of security. In future, this work can be extended by some optimization and computing techniques; hard computing techniques with agent setup and soft computing techniques with cryptographic algorithms. Efficient secure routing is promised in this paper.

References

[1] Ramesh, S., Praveen, R., Indira, R. and Ganesh Kumar, P. (2012) A Survey on Routing Methodologies for ICMANET. *Proceedings of the 4th IEEE International Conference on Advanced Computing*, Chennai, 13-15 December2012, 1-6. http://dx.doi.org/10.1109/icoac.2012.6416801

[2] Perkins, C. and Royer, E. (1999) Ad Hoc On-Demand Distance Vector Routing. *Proceedings of the 2nd IEEE Workshop on Mobile Computing Systems and Applications*, New Orleans, 25-26 February 1999, 90-100. http://dx.doi.org/10.1109/mcsa.1999.749281

[3] Ramesh, S. and Indira, R. (2015) Secure Agent Based Routing for ICMANET. *International Journal of Applied Engineering Research*, **10**, 4864-4871.

[4] Cokuslu, D. and Erciyes, K. (2008) A Flooding Based Routing Algorithm for Mobile Ad Hoc Networks. *IEEE 16th. Int. Conf. SIU* 2008, Aydin, 20-22 April 2008, 1-5.

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

[6] Spyropoulos, T., Psounis, K. and Ragavendra, C.S. (2008) Efficient Routing in Intermittently Connected Mobile Networks: The Single-Copy Case. *IEEE/ACM Transactions on Networking*, **16**, 63-76. http://dx.doi.org/10.1109/TNET.2007.897962

[7] Spyropoulos, T., Psounis, K. and Ragavendra, C. (2008) Efficient Routing in Intermittently Connected Mobile Networks: The Multiple-Copy Case. *IEEE/ACM Transactions on Networking*, **16**, 77-90. http://dx.doi.org/10.1109/TNET.2007.897964

[8] Spyropoulos, T., Psounis, K. and Raghavendra, C.S. (2005) Spray and Wait: An Efficient Routing Scheme for Intermittently Connected Mobile Networks. *Proceedings of the 2005 ACM SIGCOMM workshop on Delay-tolerant networking*, Philadelphia, 22-26 August 2005, 252-253. http://dx.doi.org/10.1145/1080139.1080143

[9] Lindgren, A., Doria, A. and Schelen, O. (2004) Probabilistic Routing in Intermittently Connected Networks. *Proc. SAPIR*, **3126**, 239-254. http://dx.doi.org/10.1007/978-3-540-27767-5_24

[10] Shi, K. (2010) Semi-Probabilistic Routing in Intermittently Connected Mobile Ad Hoc Networks. *Journal of Information Science and Engineering*, **26**, 1677-1693.

[11] Ramesh, S., Indira, R., Praveen, R. and Ganesh Kumar, P. (2013) S-Spray Routing Protocol for Intermittently Connected Mobile Networks. *ICTACT Journal on Communication Technology*, **4**, 761-765.

[12] Wen, H., Liu, J., Lin, C., Ren, F., Li, P. and Fang, Y. (2011) A Storage Friendly Routing Scheme in Intermittently Connected Mobile Networks. *IEEE Transactions on Vehicular Technology*, **60**, 1138-1149. http://dx.doi.org/10.1109/TVT.2011.2104378

[13] Saffari, M.H. and Mahjoob, M.J. (2009) Bee Colony Algorithm for Real-Time Optimal Path Planning of Mobile Robots. *IEEE*, Famagusta, 2-4 September.2009, 1-4.

[14] Rahim, M.A., Musirin, I., Abidin, I.Z., Othman, M.M. and Joshi, D. (2010) Congestion Management Based Optimization Technique Using Bee Colony. 4*th International Power Engineering and Optimization Conference* (*PEOCO*2010), Shah Alam, 23-24 June 2010, 184-186. http://dx.doi.org/10.1109/peoco.2010.5559247

[15] Wong, L.-P., Low, M.Y.H. and Chong, C.S. (2008) A Bee Colony Optimization Algorithm for Travelling Salesman Problem. *IEEE*, 2*nd International Conf. on Modelling and Simulation*, Kuala Lumpur, 13-15 May 2008, 818-823.

[16] Zhang, Y., Liu, W., Lou, W. and Fang, Y. (2006) Securing Mobile Ad Hoc Networks with Certificateless Public Keys. *IEEE Trans., Dependable and Secure Computing*, **3**, 386-399. http://dx.doi.org/10.1109/TDSC.2006.58

[17] Dhurandher, S.K., Obaidat, M.S., Verma, K., Gupta, P. and Dhurandher, P. (2011) FACES: Friend—Based Ad Hoc Routing Using Challenges to Establish Security in MANETSs Systems. *IEEE Systems Journal*, **5**, 176-188. http://dx.doi.org/10.1109/JSYST.2010.2095910

[18] Ramesh, S. and Ganesh Kumar, P. (2014) BCR Routing for Intermittently Connected Mobile Ad Hoc Networks. *International Journal of Engineering and Technology*, **6**, 66-74.

[19] Keranen, A., Karkkainen, T. and Ott, J. (2010) Simulating Mobility and DTNs with the ONE. *Journal of Communication*, **5**, 92-105.

[20] Grgen, D., Hiedels, H.F. and Jane, C. (2007) The Java Ad Hoc Network Development Environment. 40*th Annual Simulation Symposium*, Norfolk, March 2007, 163-176.