International Journal of Future Generation Communication and Networking
Vol.6, No.6 (2013), pp.61-70
http://dx.doi.org/10.14257/ijfgcn.2013.6.6.07

Secure Dominating Set-Based Routing Porotocol in MANET: Using Reputation

Amin Mohajer*, Ehsan Noori Ghalenoo, Rashin Saboor and Rahim Pasha Kianbakht

Integrated Network Management Group, Cyber Space Research Institute (CSRI)
Tehran, Iran
a.mohajer@ieee.org

Abstract

Mobile ad-hoc networks (MANETs) face a number of challenges, in particular due to its dynamic network topology. A self organizing framework can overcome the problems associated with changing topology and dynamic behavior of mobile nodes thus routing has become a great challenge to these types of networks. Such a framework can be created by using connected dominating set (CDS). But the choice of misbehaving node as CDS will inversely affect the network performance. A misbehaving node may disturb the network by denying packet forwarding. In this paper we propose a new reputation based routing protocol using CDS (Connected Dominating Set). The proposed weight heuristic is applied to each node in network for selecting CDS based on uses the reputation value in order to selective forwarders detection. Reputation refers to the opinion of one node about another node. Hence only well behaving and good quality nodes are selected as a dominant node for CDS construction. Through simulation results proves that the proposed method performs well compared to MPR selection approach in OLSR.

Keywords: *CDS, Mobile Ad-Hoc Network, Reputation, Self-Organization*

1. Introduction

Today, mobile networks are increasingly popular because of its low cost and convenient deployment. These networks provide speedy access to information for all users independent of their location. Mobile networks are divided into two main categories: cellular networks and ad-hoc networks. The cellular networks are characterized by a fixed infrastructure and ad-hoc networks are characterized by infrastructure less architecture. Mobile Ad-hoc Network (MANET) is a self-configuring wireless networks which consist of several mobile nodes. The nodes are free to move randomly in any direction, so they have no infrastructure.

Each and every mobile node can act as a router, client or both. The main characteristics of MANET includes: Self-organizing, self-restoring, fully decentralized, and highly dynamic network topology. Self-organization of an ad-hoc network creates a topology called virtual structure. These systems are more robust against failures and damages [1]. They are adaptable to the dynamic environment. This framework creates a hierarchy between the most strong and most weak nodes. The aim of this paper is to develop a secure routing protocol reputation value which uses a weighting heuristic.

The specific interest here is on the access to the network layer functionalities like routing and packet forwarding. Access should be given only to well-behaving nodes and not to misbehaving nodes. A misbehaving node can be malicious node. A malicious node may enjoy

[*] Corresponding Author

ISSN: 2233-7857 IJFGCN

network services, *e.g.*, receiving packets destined for itself but refuse to route or forward packets for others, therefore invalidating the basic collaboration premise in almost all current routing algorithms for mobile ad-hoc networks. A malicious node may seek to damage or disrupt normal network operations. Moreover, misbehaving node may act as a good network citizen for a certain time period or in certain places, but then starts to act maliciously at other times or locations.

This paper is organized as follows. Section II describes related works associated with CDS construction. In Section III, we present a reputation based method for CDS construction. Section IV gives simulation results. Finally Section V concludes the paper.

2. Related Works

All The nodes in a mobile ad-hoc network are categorized into dominant nodes (CDS nodes) and dominatee nodes. The connected structure of the dominant nodes creates a virtual backbone or a Connected Dominating Set (CDS). The adjacent nodes of dominant nodes are called dominatee nodes. The messages transmitted by using this virtual backbone effectively reduce the communication overhead. The selection strategy of dominant node for connected dominating set construction is different for different approaches.

J. Wu and H. Li [2] proposed a simple and efficient algorithm for calculating the connected dominating set in a connected graph, which represents the scenario for a mobile ad-hoc wireless network. In this paper they proposed a marking process that marks every vertex in a connected and un-weighted graph. A node is marked as dominant if two of its neighbors are not directly connected. To reduce the size of a connected dominating set, they proposed two rules.

RULE 1: If *u* and *v* are two vertices in a graph G, and *id(u) < id(v)*, then a marked node '*u*' can unmark itself if the marked node '*v*' covers it.

RULE 2: A marked node can unmark it, if it is covered by two other directly connected marked neighbors.

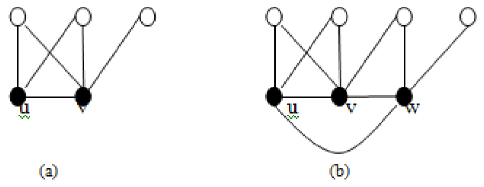

Figure 1: Two Samples

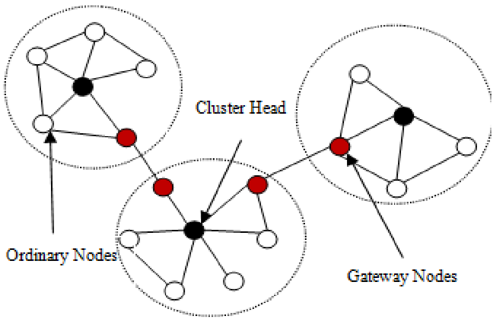

Figure 2: Clustering

In Figure 1(a), since *N(v) N(u)* and *id(v) < id(u)}*, then the node *v* can unmark itself. In Figure 1(b), the node *v* can unmark itself because of *N(v) N(u) N(w)* and *id(v)=min{id(v),id(u),id(w)}*. Wu and Li's approach performs well for finding a small dominating set than any other classical approaches. Each node gets its neighborhood information and their status (mark or unmark) by exchanging Hello messages. So it imposes communication overhead and high energy consumption. The main advantage of connected dominating set is that the routing information is localized to adapt the topological changes.

I. Stojmenovic *et al.*, [3] improves the construction of CDS by replacing the node id with a key (*degree,x,y*), where *degree* is the number of neighbors of a node, *x* and *y* are its coordinates in the plane. Each node compares its degree with the degree of neighboring nodes. A node with higher value of degree has the chance of being a dominant node. The new broadcasting algorithm reduces the ratio of dominant nodes and eliminates the neighbor that already received the message. The main characteristics of this algorithm are reliability, parameter less behavior and rebroadcast saving.

X.Cheng and D.Du [4] proposed two algorithms for building and interconnecting the dominating set. Algorithm I is cost aware. Algorithm II is degree aware. A node has one of four following states: initial state, dominant (CDS member), dominatee (neighbor of a dominant) and active (in election). Each host maintain some parameters such as *dom, rank*. *dom* represents the dominator and *rank* defines the virtual relationship among neighborhood. These parameters are updated by exchanging three messages: <*dominant (u,dom,rank)* >,<*dominatee (u,dom,rank)*> , <*active(u)*>. Initially all host belongs to initial state. The leader node goes to dominant state and neighbor becomes dominatee. An active node that has the smallest *(cost, id)* among all its active neighbors becomes a dominant node. In algorithm II an active host with maximum effective degree among all its active neighbors becomes dominant node. The backbone optimizes flooding: only the members in dominating set forward the control packets, reducing the global load, and allowing other nodes to spare their energy.

Another method for CDS framework is based on clustering. In the cluster-based category, the nodes are grouped into a set of clusters [5]. Generally in each cluster, a specific node called leader or Cluster-Head (CH) is designed to organize the set of specific functionalities within its cluster. The clusters are identified by the identity of the Cluster-Head. If the Cluster-Head fails, then the cluster no longer exists. A gateway node is one with at least two Cluster-Head as neighbors. The gateway node acts as a boundary node for each cluster. All other nodes belonging to a cluster are called Ordinary nodes. Figure 2 depicts a cluster framework which consists of Cluster-Head, gateway and ordinary nodes. Cluster-Head schedules transmission and allocates resources within its cluster.

F. Theoleyre and F. Valois [6] proposed a virtual structure which consists of three phases: Neighborhood Discovery, Cluster formation, Backbone creation. Neighborhood discovery is performed by sending HELLO messages. The cluster formation and Cluster-Head election is done by a distributed election and forms a cluster of radius $K_{cluster}$. A node moving inside a cluster does not make any topology changes. The Cluster-Heads and gateway nodes together form a CDS structure. The distance from a node to the backbone is at most k_{cds} hops. A backbone helps to collect control traffic and to reduce overhead of route discovery. The integration of stable cluster formation and backbone creation creates an infrastructure that adapts to topological changes.

Ali Kies *et al.*, [7] presents a self organization framework based on weight parameter. Here the distance between the dominant node and dominate node is one hop. It is to limit the disconnection in the network. The weight parameter depends on quality of link, energy and connectivity. Eq. 1 depicts the weight parameter.

$$P\ selection = \alpha . D\ +\ \beta . E\ + \gamma . M \qquad (1)$$

where:

D: is the degree of the node
E: represents the remaining energy level
M: is the received signal strength
α, β and γ are the weighting factor.

To build the connected dominating structure, it acquires neighborhood knowledge by using the HELLO messages. In this approach, the dominant nodes have high energy, strong neighborhood and good quality of signal. This will help to avoid the frequent disconnection. But the problem with CDS construction is that the choice of misbehaving node as the dominant node will affect the network performance.

3. Proposed CDS Model: RPROC

The proposed CDS model is based on a reputation value which uses a weighting heuristic. Hence it is named as RPROC (Reputation based Proactive CDS) .The weighting heuristic depends upon energy, degree, willingness and reputation factor of each node. This helps to reduce energy consumption, and thereby increasing the survivability of the network. Also, this approach reduces the number of dropped packets and provides secure routing protocol.

3.1. Selective Forwarding Attack

Selective forwarding occurs when a malicious node refuses to forward certain packets and simply drops them. One of the easiest ways of trying to influence the communication in a Multihop network is selective forwarding. Even without knowing anything about the contents of the messages, this attack can be effective.

Even in protocols completely resistant to sinkholes, wormholes, and the Sybil attack, a compromised node has a significant probability of including itself on a data flow to launch a selective forwarding attack if it is strategically located near the source or a base station

3.2. Reputation

Reputation is the opinion of a node about another node. Reputation based frameworks helps to analyze the behavior of a node *i.e.*, Whether the node is misbehaving or well-behaving by analyzing the previous history of a node. This reputation system can be used to make decisions about which nodes to include and which nodes to exclude from the network.

3.3. Reputation Factor Estimation

The estimation of reputation value [8] of a node helps to classify a node as well behaving or misbehaving. Suppose a mobile ad-hoc network consist of 'N' nodes. Each node calculates reputation value of its neighbors by using Eq.2.

$$(RN_{direct})_t = \frac{PDR}{PRR} \qquad (2)$$

where RN_{direct} is the reputation value calculated by monitoring the neighbors directly in time t that is when nodes can detect misbehaving nodes periodically. The node C_i considers node d_{ik} as selective forwarders if the dropping ratio of d_{ik}, *i.e.*, ratio of a number of packets dropped (PDR) to a number of packet received (PRR), is higher than a predefined threshold.

If the reputation value of a node is greater than 0.8, then it is a miss behaving node. This node cannot be chosen as a dominant node.

3.4. Weighting Factor Estimation

The weight parameter depends on degree, energy, quality of the link, and reputation value. Eq. 3 depicts the weight parameter.

$$WF = \begin{cases} X1 = D + E + WL \\ X2 = RN \end{cases} \quad (3)$$

where:

WF: is the weighting factor
D: is the degree of the node
E: represents the remaining energy level
WL: is the willingness of a node to become CDS
RN: is the reputation factor

We select nodes that have the highest X1 and their X2 are less than 0.8

3.5. Heuristic for CDS Selection

The purpose of this CDS selection algorithm is to identify well behaving nodes as CDS and thereby optimizing the control overhead. In our reputation based system, there are two phases: Well-behaving node discovery based on the reputation value (X2) of an CDS construction based on the weight heuristic (X1). In this section we describe about proposed heuristics for CDS selection based on a weight factor and reputation value. The proposed CDS heuristic is applied to each node x in network G as shown in Figure 3. The following terminologies will be used in describing the algorithm.

RN(x) A set of neighbors of node ‘x’ which can have the reputation value less than 0.8

R(x) Set of reachable nodes from N1 to N2

CDS(x) CDS of node ‘x’.

N1 A set of 1 hop neighbors.

D(x) A degree set of 1 hop neighbor of node ‘x’.

E(x) Energy set of 1 hop neighbor of node ‘x’.

WF(x) The weight factor of 1 hop neighbor of node ‘x’ WF(x) = $D_i + E_i + WL_i + RN_i$

D_i Degree of a node i (i is a member of N1)

E_i Energy of a node i (i is a member of N1)

WL_i Willingness of a node i (i is a member of N1)

RN_i	Reputation value of a node i

```
Heuristic CDS(G = (V,E); N1; N2; R(x);RN(x) ⊂ V; CDS(x) ⊂ V )
Step 1      Initially, set CDS(x) = {}, R(x)={} and RN(x) = {}.
Step 2      For each node in N1, calculate the reachability. i.e. nodes in N2 which are
            reachable through N1. Add those nodes in the set R(x)
Step 3      While there exist nodes in R(x) :
    Step 3.1    For each node in R(x), calculate the reputation factor R(x) and add node with
                reputation value less than 0.8 to RN(x).
    Step 3.2    For all nodes in RN(x), calculate D(x),E(x),WL(x) ∀y ∈ RN(x), where D(x) is
                the degree of the node, E(x) is the energy of the node and WL(x) is the
                willingness of the node to become a CDS.
    Step 3.3    Calculate the weight WF(x), where $WF(x) = D_i + E_i + WL_i + RN_i$
    Step 3.4    Add node in RN(x) that provide the highest weighted WF(x) to CDS(x)
    Step 3.5    If a tie case occurs in above step then Add node with maximum energy E(x)
                to the CDS (x).
    Step 3.6    If a tie case occurs in above step then Add node with maximum degree D(x)
                to CDS(x).
Step 4      Stop
```

Figure 3. Heuristic for CDS Selection Process

In this algorithm, CDS selector selects the well behaving node as dominant node. In step 2, it identifies the nodes that have connectivity from N1 to N2. This helps to avoid the unnecessary calculation of non-reachable nodes. Then it calculates the reputation value of all nodes which belonging to R(x). Nodes can have a reputation factor less than 0.8 are added to the set RN(x). Calculate the weighing factor of every neighboring node which belongs to the set RN(x). In step 3, CDS selector selects the node having highest weighing factor as dominant node. If there is any tie (two or more nodes with the same value of weighing factor), a node with maximum remaining energy will be chosen. In addition if there is another tie, node which provide highest degree value will be selected as CDS node.

3.6. Dominating Set-Based Routing in MANET Networks Using Reputation

The proposed approach is implemented over the Dominating-set-based Routing. Reputation value of node is used to classify a node as well behaving or misbehaving. Each node uses a monitoring mechanism like "watchdog" to monitor their neighbors. Monitoring the neighbors helps each node to calculate the reputation value of each of its neighbor.

The main advantage of dominating-set-based routing is that it simplifies the routing process to one in a smaller subnetwork generated from the connected dominating set. This means that only gateway hosts need to keep routing information. As long as changes in network topology do not affect this subnetwork, there is no need to recalculate routing tables.

Clearly, the efficiency of this approach depends largely on the process of finding and maintaining a connected dominating set and the size of the corresponding subnetwork.

The routing process can be divided into steps:

1. If the source is not a gateway host, it forwards the packets to a source gateway, which is one of the adjacent gateway hosts.
2. This source gateway acts as a new source to route the packets in the induced graph generated from the connected dominating set.
3. Eventually, the packets reach a destination gateway, which is either the destination host itself or a gateway of the destination host. In the latter case, the destination gateway forwards the packets directly to the destination host.

4. Simulation Results

We conducted simulations using NS2 [9], to determine the effectiveness of our proposed CDS heuristic and compare it with the MPR [10] selection approach in OLSR [11] routing protocol. Nodes are moving according to the Random Waypoint mobility Model (RWP). In RWP mobility model [12], the nodes have a non uniform spatial distribution. Table 1, gives the simulation parameters.

TABLE I SIMULATION PARAMETERS

Parameter	Value
Number of nodes	20-50
Simulation Time	100s
Radio range	250m
Velocity	2-10 m/s
Simulation area	500 X 500 m^2
MAC	IEEE 802.11b
Initial energy	1000 Joules
Transmission Power	1.4 W
Reception Power	1.2 W
Idle Power	0.9 W
Traffic Type	CBR
Packet Size	512 Bytes

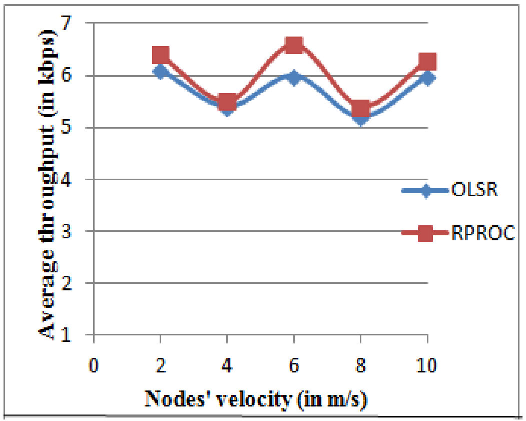

Figure 4: Throughput vs. Velocity

To evaluate the performance of our heuristics, we focused on three performance parameters: Average throughput, Packet delivery ratio and average end-to-end delay by considering nodes density, mobility and the number of traffic connection. For each scenario we performed random simulations. The performance metrics are described as follows:

- Average throughput: the amount of data that are delivered per second over the network

- Packet delivery ratio (PDR): the ratio of total number of packets received by destinations to total number of packets sent by sources

- Average end-to-end delay: the average amount of time for all packets to reach destination

The speed of the nodes is varied for studying the performances of our algorithm in a highly dynamic topology since node movement seems to be an important metric in determining the performance of ad-hoc routing protocols. Figure 4 shows that, the CDS heuristic algorithm performed better than traditional OLSR .The low throughput of OLSR is due to the broken links between nodes. In the CDS heuristics the links are established by considering the connectivity, degree and energy of a node by using a weight factor. It helps to improve the survivability of the network.

PDRs of the two protocols are demonstrated in Figure 5. Reputation based proactive CDS has the highest PDR than OLSR, because stable and better nodes are selected as CDS nodes, based on a weighing factor which uses the reputation value. This avoids misbehaving nodes and thus results in a higher packet delivery ratio. End-to-end delays of each protocol are highlighted in Figure 6. The delay of RPROC is lesser than OLSR since it considers a weighing factor in the CDS computation process. The weighing factor helps to discover stable links for packet forwarding.

Figure 7 shows that PDR of OLSR decreases with increasing node density. Since misbehaving nodes are eliminated and nodes with highest weight factor are selected for packet forwarding, RPROC increases the CDS lifetime. Hence dropping of packet is less in RPROC compared to OLSR. Figure 8 shows delay with the number of nodes. According to figure 8, RPROC have lower delay than OLSR as there will not be any broken links between the CDS nodes.

Figure 9 compares the PDR of protocols by varying the number of traffic connections. The PDR of RPROC is much better than OLSR. It is above 98%, while OLSR provide only 93%. The increase in the rate of traffic connection will not inversely affect the delivery of packets in RPROC. In Figure 10, the average throughput of RPROC is greater than that of OLSR because it limits the dropping of packet by introducing reputation weight factor.

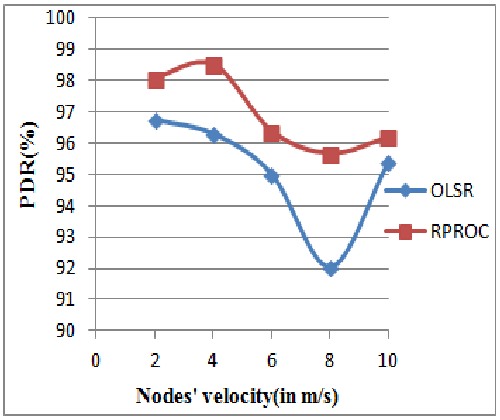

Figure 5: PDR vs. Velocity

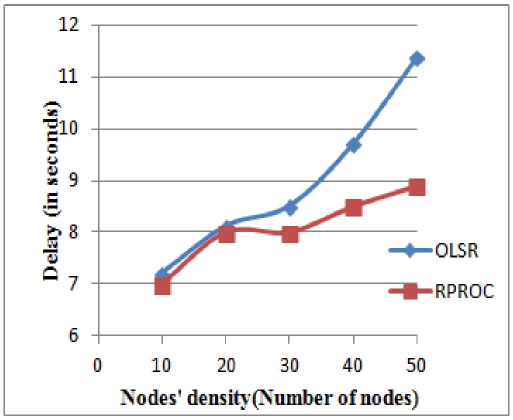

Figure 8: Delay vs. Density

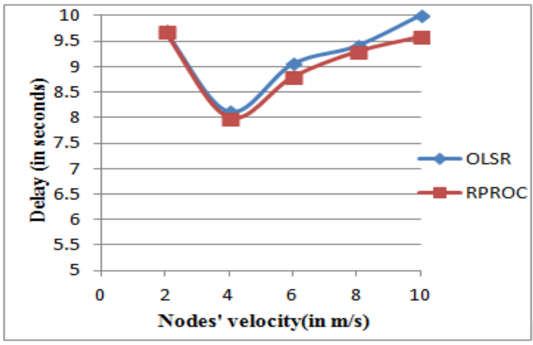

Figure 6: Delay vs. Velocity

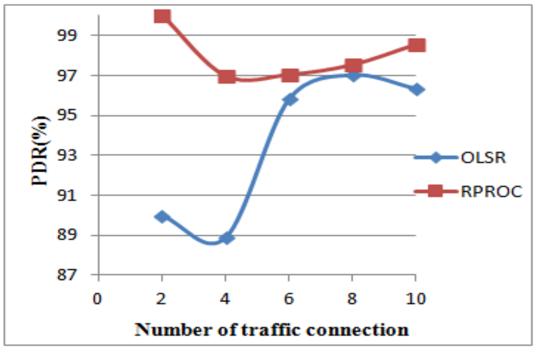

Figure 9: PDR vs. Traffic

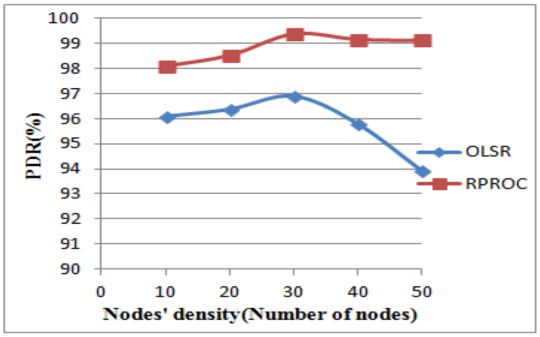

Figure 7: PDR vs. Density

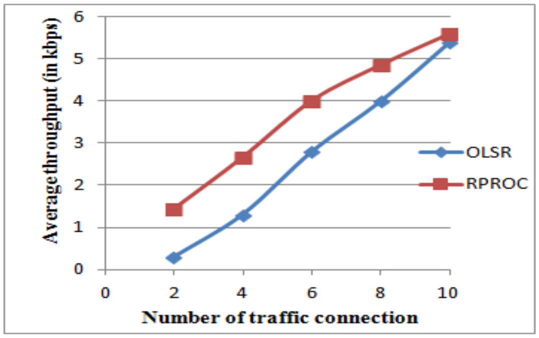

Figure 10: Throughput vs. Traffic

5. Conclusion

The In this paper, we proposed a routing protocol based on secure CDS model for mobile ad-hoc networks based on a reputation value which uses weighing heuristic. The weighting heuristic also depends upon the energy, willingness and degree of a mobile node. The weighting heuristic helps to identify the best and well behaving nodes for the construction of safe CDS because the malicious dominant node will inversely affect the network performance. Here the nodes having highest weight factor and reputation value less than 0.8 are selected as CDS node. This helps to increase the survivability of the network. The simulation results show that our CDS model have high packet delivery ratio, high throughput and low delay than existing proactive protocol such as OLSR.

Acknowledgements

This work was supported by Iran Telecommunication Research Center (ITRC).

References

[1] K. L. Mills, “A brief survey of self-organization in wireless sensor networks”, Wireless Communications and Mobile Computing, vol. 7, **(2007)** September.

[2] I. Stojmenovic, M. Seddigh and J. Zunic, “Dominating sets and neighbor elimination based broadcasting algorithms in wireless networks”, IEEE Transactions on Parallel and Distributed Systems, vol. 15, **(2004)** November.

[3] S. Sangheethaa, J. Venkatesh and A. Korath, “Reputation based Dynamic Source Routing Protocol for MANET”, International Journal of Computer Applications (0975 – 888) 07/2012, vol. 47, pp. 975-888.

[4] X. Cheng and D. Du, “Virtual backbone-based routing in multihop ad-hoc wireless networks”, Technical Report 02-002, University of Minnesota, Minnesota, USA, **(2002)** January.

[5] Network Simulator NS2, http://www.isi.edu/nsnam/ns/index.html.

[6] A. Qayyum, L. Viennot and A. Laouiti, “Multipoint Relaying: An Efficient Technique for Flooding in Mobile Wireless Networks”, INRIA Research Report RR-3898, **(2000)**.

[7] T. Clausen and P. Jacquet, “Optimized Link State Routing Protocol (OLSR)”, RFC 3626, IETF Network Working Group, http://www.ietf.org/rfc/rfc3626.txt, **(2003)** October.

[8] J. Wu and H. Li, “On calculating connected dominating set for efficient routing in ad-hoc wireless networks”, 3rd Int’l Workshop on Discrete Algorithms and Methods for Mobile Computing and Communication (DIAL'M), Seattle, USA, **(1999)** August.

[9] B. Haggar, “Self-Stabilizing Clustering Algorithm for Ad-hoc Networks”, The Fifth International Conference on Wireless and Mobile Communications, ICWMC 2009, French Riviera, France, **(2009)** August.

[10] F. Theoleyre and F. Valois, “Virtual structure routing in ad-hoc networks”, IEEE ICC’2005, Seoul, Korea, **(2005)** May.

[11] K. Ali, M. Sara, R. Belbachir, Z. Mekkakia Maaza and S. Mohammed Senouci, “Self-organization Framework for Mobile Ad-hoc Networks”, 8 th Int’l conference on Wireless Communications and Mobile Computing, **(2012)** August.

[12] J. Y. Le boudec and M. Vojnovic, “Perfect Simulation and Stationarity of a Class of Mobility Models”, proceedings of ieee infocom, vola, **(2005)** March, pp. 2743-2754.

Authors

Amin Mohajer, received the B.S. degree in Electronics and Electrical Engineering from Shahed University, Tehran, Iran in 2008. He is working toward the M.S. Degree in Electrical and Secure Communication Engineering with Mobile Ad-Hoc Networking Laboratory, School of Information and Communication Technology, Malek ashtar University of Technology, Tehran, Iran. His areas of research include Mobile Ad-Hoc Networks, Network Coding, Linear Communications, Cognitive Radio Networks, and cryptography.

Ehsan Noori, received the B.S. degree in Electronics and Electrical Engineering from Islamic Azad university, Karaj, Iran, in 2008. He is working toward the M.S. Degree in Electrical Engineering- Communications System, with Mobile Ad-Hoc Networking Laboratory, School of Information and Communication Technology, Malek ashtar University of Technology, Tehran, Iran. His areas of research include Wireless Networking, Mobile Ad-Hoc Networks, Wireless sensor networks, and Cognitive Radio.

Rashin Saboor, received the B.S. degree in Electronics and Electrical Engineering from Shariaty College, Tehran, Iran in 2008. She is working toward the M.S. Degree in Electrical and Secure Communication Engineering with Mobile Ad-Hoc Networking Laboratory, School of Information and Communication Technology, Malek ashtar University of Technology, Tehran, Iran. Her areas of research include Mobile Ad-Hoc Networks, Cognitive Radio Networks, and cryptography.

Rahim Pasha Kianbakht, received the B.S. degree in Electrical Engineering, Communication Systems from Raja University, Qazvin, Iran. His areas of research include GSM, communications systems, mobile ad-hoc networks, distributed wireless networks, digital communications.