PB-OLSR: Performance Based OLSR

Mohamed DYABI, Abdelmajid HAJAMI, Hakim ALLALI
LAVETE Laboratories

University of science and Technology *Settat, Morocco*

Abstract: ***Ad hoc network consists of mobile nodes which communicate with each other through wireless medium without any fixed infrastructure. As a result, to ensure routing service, nodes must act as a router. If one of them is malicious, it would represent a threat against the security of the network. The router role is resource consuming since it's always switched on and is responsible for the long-range transmission. to send a bit over 10 or 100 m distance, Manet's nodes consume resources that can perform thousands to millions of arithmetic operations. It is here that our work gives great importance to node performance and trust. This work consists of two parts: The first one is to propose a model to measure the performance and the trust of network nodes, and the second part is to improve network performance by the integration of a new version of OLSR protocol, (PB-OLSR).***

Keywords: Adhoc, Olsr, Mpr, Trust**.**

1. Introduction

Mobile Ad-hoc NETwork (MANET) is a collection of mobile wireless devices that are able to communicate without any pre-established network infrastructure. To ensure routing service, all nodes in MANET cooperate in forwarding neighbor's traffic until reaching its intended destination. Traditional routing protocols built for wired networks could not be directly used in MANETs. This is because MANETs are characterized by many challenging features including poor wireless-link quality, node mobility, and limited resources. This is in addition to the lack of any central control. Due to the above-mentioned features, the design of specific routing solutions for MANETs has made the main focus of almost all researchers' contributions in the field of mobile ad hoc networking [1].

Routing protocols for MANETs could be classified as either reactive or proactive [2]. A reactive routing protocol does not calculate routes beforehand, but only when data traffic is present for routing. This is done via a route discovery procedure which is initiated by the source node. This latter broadcasts a Route REQuest (RREQ) packet to all its one-hop neighbors. Each neighboring node rebroadcasts again the received RREQ. The same operation is repeated until that destination node is reached. In answer, the destination node generates a Route REPlay (RREP) packet. This approach presents the disadvantage of a long response time in comparison to its proactive counterpart.

Proactive routing protocols, also known as table driven, are modifications of traditional link-state and distance vector based routing protocols for wired networks. They are built on periodic exchange of routing information. This is in the aim of making routing tables up to date all the time. Moreover, routes are maintained toward all possible destinations. Hence, routing could start immediately whenever data traffic is present. However, the main drawback of proactive routing is the great amount of generated routing overhead. This leads to the wastage of network-bandwidth and nodes-resources.

One interesting proposal to reduce the generated routing overhead by the proactive approach is the concept of Multi-Point Relays (MPRs) introduced in the OLSR protocol [3]. The key idea is to limit the number of retransmissions required for a node to flood a packet in the entire network. For this purpose, each node elects a subset of its one-hop neighbors to be responsible of forwarding its broadcasted packets. Those nodes are called MPRs.

The MPR role is resource consuming since it's always switched on and is responsible for the long-range transmission. to send a bit over 10 or 100 m distance, Manet's nodes consume resources that can perform thousands to millions of arithmetic operations

Certainly such a solution minimize the overall network resources consumption. However, OLSR overuses the resource of the MPRs nodes. In fact, resources are drained more quickly in MPRs nodes than in no-MPRs ones. Therefore, it is a mandatory to rethink resources aware versions for the OLSR protocol. Particularly, maximum lifetime routing approach that avoids nodes with poor resources profiles should be adopted.

Security is also a big challenge in the MPR selection, if the MPR node is malicious, it would represent a threat against the security of the network.

It is here that our work gives great importance to nodes performance and reputation.

This work consists of two parts: The first part is to propose a model to measure the performance and the reputation of nodes. The second part attempts to improve network performance by the integration of a new version of OLSR protocol (PB-OLSR).

Manuscript received April 5, 2015
Manuscript revised April 20, 2015

The paper is organized as follows. In Section 2, an overview of OLSR is presented. In Section 3, related works on security in ad hoc networks are summarized. In Section 4, we present the performance and trust computation, then we present the Performance based OLSR in Section 5. Finally, we conclude this paper by presenting simulation results and our future works.

2. THE OLSR PROTOCOL

The optimized link state routing (OLSR) protocol [4] is a proactive routing protocol that employs an efficient link state packet forwarding mechanism called multipoint relaying.

Optimizations are done in two ways: by reducing the size of the control packets and also by reducing the number of links that are used for forwarding the link state packets. The reduction in the size of link state packets is made by declaring only a subset of the links in the link state updates. The subset neighbors that are designated for link state updates are assigned the responsibility of packet forwarding are called multipoint relays.

The optimization by the use of multipoint relaying facilitates periodic link state updates. The link state update mechanism does not generate any other control packet when a link breaks or when a link is newly added. The link state update optimization achieves higher efficiency when operating in highly dense networks. The set consisting of nodes that are multipoint relays is referred to as MPRset. Each given node in the network elects an MPRset that processes and forwards every link state packet that this node originates. Each node maintains a subset of neighbors called MPR selectors, which is nothing than the set of neighbors that have selected the node as a multipoint relay. A node forwards packets that are received from nodes belonging to its MPRSelector set. The members of both MPRset and MPRSelectors keep changing over time. The members of the MPRset of a node are selected in such a manner that every node in the node's two hop neighborhood has a bidirectional link with the node.The selection of nodes that constitute the MPRset significantly affects the performance of OLSR. In order to decide on the membership of the nodes in the MPRset, a node periodically sends Hello messages that contain the list of neighbors with which the node has a bidirectional link. The nodes that receive this Hello packet update their own two hop topology table. The selection of multipoint relays is also indicated in the Hello packet. A data structure called neighbor table is used to store the list of neighbors, the two-hop neighbors, and the status of neighbor nodes. The neighbor nodes can be in one of the three possible link status states, that is, unidirectional, bidirectional, and multipoint relay.

The algorithm allows each node to build all of its MPR is defined as follows:

X: node performing the computation.
N: set of neighboring nodes of x.
N2: all 2-hop neighbors, excluding:
- Nodes only accessible by members of N with willingness = WILL_NEVER
- The node x itself.
- All the symmetrical neighbors of node x .

MPR_Set: set of all MPR for the node x.
D(v): he degree of node v (where v in N), which is the number of symmetric neighbors nodes of v,
Except of:
- All the members of N
- The node x itself

The algorithm:

1. Add to MPR_Set all nodes v Where v is in N and v_willingness = WILL_ALWAYS
2. Whatever v in N calculate D(v)
3.
   3.1. Add to MPR_Set any node v where v in N and v is the only node to reach nodes in N2
   3.2. Delete from N2 any node w currently covered with MPR_Set.

4. While N2! ={}
   4.1. Whatever v in N compute: reachability (v) (reachability (v) is the number of N2 nodes that are not yet covered by at least one node in the set MPR_Set, and are accessible via this node v.

   4.2. Add to MPR_Set any node v of N which r>0 & max(willingness)
   If this presents several choices, select the v that max (r)

   If multiple choices are present, select the v that max (D)

   4.3. Remove all nodes w where w Î N2 and w is currently covered by MPR_Set
5. The end of while.

In OLSR, only nodes selected as MPRs broadcast messages on the status of links. The aim is to obtain the smallest number of MPRs suitable to cover the entire network. Moreover, the OLSR uses 4 types of control messages [5]:

- HELLO: used for neighbor detection.
- TC (Topology Control): diffuse topology information.
- MID (Multiple Interface Declaration) can publish a list of interfaces on each node

- HNA (Host and Network Association): used to declare the subnets and hosts (excluding MANET) reached by a node acting as a gateway.

Thus, OLSR performs two main actions:

- The first is the detection of near by sending HELLO messages and determining The MPR.
- The second is the topology management. It is made by the intervention of TC messages, MID and HNA and results in a global routing table in each entity.

3. RELATED WORK

In the literature, several studies have addressed the problem of maximizing the routing lifetime for OLSR protocol, very intuitively, Ghanem et al. [6] proposed to use the residual energy as a criterion for choosing MPRs nodes. In addition to the residual energy, Wardi et al. [7] suggested considering the reachability and the degree of one-hop neighbor nodes. To select paths with maximum bottleneck residual energy level, Benslimane et al. [8] combined energy-aware MPR selection with an energy aware path determination algorithm. Guo et al. [9] modified the path computing algorithm in OLSR. Paths are selected according to the residual energy level of intermediate nodes. Mahfoudh et al. [10] proposed a variant of OLSR where MPR selection and path calculation is determined by both a node's residual energy level and its number of neighbors. De-Rango et al. [11] modified the setting method of the willingness parameter in OLSR. This is by introducing the battery power and the expected residual lifetime. In the same context, Lakrami et al. [12] suggested considering energy and mobility factors.

for the purpose of securing the Adhoc network, Michiardi et al. propose a cooperation enforcement mechanism, called CORE (COllaborative REputation) [13]. Basically, CORE allows each device to monitor its neighbors. Based on its own observation as well as the scores provided by other devices involved in the current operation, a device can compute a reputation score for each of its neighbors, this score represents the degree of cooperation. Buttyan and Hubaux have proposed the collaboration mechanism, called Nuglets [14] adopting a completely different approach. They introduce a virtual currency called nuglet. Each node has to pay to use network services (forwarding its data), and must be paid for offering services to other nodes. Thus, selfish nodes will finish their nuglets and can no longer send packets.The drawback of this method is that the nuglets are managed by a centralized entity.

In [15], Adnane et al., proposed a trust based reasoning for OLSR that allows each node to correlate information provided by Hello, TC messages and data packets information so as to validate its local view of the global network topology. In their approach, when an inconsistency is detected between any received messages and its local view, the reasoning node is able to identify the compromised route.

Rachid Abdellaoui and Jean-Marc Robert [16] propose an approach called SU-OLSR , the approach prevent that a malicious node forces its neighbours to select it as a MPR node, indeed ,the MPR selection algorithm has to find ,first, the non-trusted nodes according to the selected criterion and, second, the trusted MPR nodes covering a maximal subset of 2-hop neighbours. Unfortunately, legitimate neighbours can be discarded if they show the same characteristics. Thus, some 2-hop neighbours may not be covered. Minor changes would have to be made to the control messages.

Our proposal presents a simple, light and quiet solution. First, our proposal does not add any new control message and the network is not overloaded or slowed at all. No changes are made to standard control messages.

MPR nodes are selected based on node performance and trust, i.e, the node that has the best reputation in the network and the best material resources such as residual energy, free memory, processor speed and hard disk space is elected as MPR.

Our algorithm takes into account the node range by including in our calculation the node density.

Therefore, we are sure that the mpr role is represented by the trustworthy, the most powerful and the densest node in the network that can perform the router roles in the best conditions.

4. PERFORMANCE COMPUTATION

A. Node Performance computation: Perfi

To calculate the performance of a node, our algorithm uses several metrics, including: Residual energy, free memory, processor speed, disk space and node density.

To determine the weight associated with each metric we used a multi-criteria analysis method [17]

3.1 Multi-criteria analysis method:

Multi-Criteria Decision Analysis, or MCDA, is a valuable tool that can be applied to many complex decisions.

It can solve complex problems that Include qualitative and/or quantitative aspects in a decision-making process.

3.2 Why use multi-criteria analysis in performance assessment:

The performance of a node is calculated based on a number of criteria that the list is not exhaustive. So far we have identified five: autonomy, density, RAM, CPU and Hard Disk associated with each node.

The global performance of the node is obtained by adding the partial performances (criteria) affected by relative weights.
In decision analysis, this operation is called synthesis or additive aggregation.
Regarding the assessment of the relative weights of the criteria, there are several Multi-criteria Decision Analysis methods. We selected Rank Order Centroïde (ROC) [18] for its simplicity and its proven efficiency.

3.3 Rank Order Centroid (ROC)

Several methods for selecting weights, including equal weights (EW) and rank-order centroid (ROC) weights, have been proposed and evaluated [19–21].
A common conclusion of these studies is that ROC weights appear to perform better than the other rank-based schemes in terms of choice accuracy.
This method is a simple way of giving weight to a number of items ranked according to their importance. The decision-makers usually can rank items much more easily than give weight to them.
The centroid method assigns weights as follows, where w1 is the weight of the most important objective, w2 the weight of the second most important objective, and so on

$$D = \left\{ W_1 \geq W_2 \geq \ldots \geq W_m \geq 0 \text{ et } \sum_{j=1}^{m} W_j = 1 \right\}$$

This method takes those ranks as inputs and converts them to weights for each of the items.
The conversion is based on the following formula:

$$W_j = \frac{1}{m}\left(\frac{1}{j} + \frac{1}{j+1} + \ldots + \frac{1}{m} \right)$$

B. Calculation of weight by the classification rank order centroid:

Step 1: Sort criteria in descending order of importance

RAUT > RDENS > RRAM > RPRO > RHDD

Step 2: fill the matrix

	RAUT	RDENS	RRAM	RPRO	RHDD	Control
R1	1,00	0,00	0,00	0,00	0,00	1,00
R2	0,50	0,50	0,00	0,00	0,00	1,00
R3	0,33	0,33	0,33	0,00	0,00	1,00
R4	0,25	0,25	0,25	0,25	0,00	1,00
R5	0,20	0,20	0,20	0,20	0,20	1,00
Avg	0,46	0,26	0,16	0,09	0,04	1,00
						1,00

Step 3: provide weights

POIDS	RAUT	RDENS	RRAM	RPRO	RHDD	Cntrl
	0,46	0,26	0,16	0,09	0,04	1,00

The column control ensures that all weights are normalized (sum of weights = 1)
After this work, the formula becomes:

RPERF = 0, 46 * RAUT + 0, 26 * RDEN + 0, 16 * RRAM+ 0, 09 * RPRO + 0, 04 * RHDD

5. TRUST COMPUTATION

OLSR protocol relies on Multipoint Relay (MPR) nodes which broadcast the topology information and forward data packets towards their destination. MPR nodes have to rely on their own resource, In terms of resource consumption, data transmission is the most expensive function in the MANET environment. To send a bit over 10 or 100 m distance, Manet's nodes consume resources that can perform thousands to millions of arithmetic operations [22]. Thus, it may not forward others' packets and simply discard them on purpose. Or they may excessively reduce transmission power to save energy, resulting in a network partitioning. Any such feature of behavior is called selfishness [23].
The selfishness is one of the attacks that threaten the functioning of the network, to elect the suitable node to act as MPR we propose to add the trust metric in our Performance computation

5.1 Trust Definition:

A standard definition considers trust to be a measure of subjective belief that one person or party uses to assess the chance another can perform a good action before the chance presents itself to observe whether or not that activity has occurred. Once an individual is taken into account trustworthy; it's meant that there's a high chance that the actions they're expected to perform are done in a way that's favorable to the trustor [24].

5.2 Trust in Manet:

In Manet trust will be outlined as a level of belief in line with the behavior of nodes [25]. In distributed ad-hoc networks, trust levels are devised from the analysis of collected knowledge from observations for specific actions of a node [26]. This might embody packet routing, wherever a node would possibly observe the routing behavior of another node. It may log that a selected node forwards some packets as traditional, and then drops other packets. It may receive this through direct neighbor sensing [27] and calculate trust from direct expertise. Trust between immediate neighboring nodes is thought as trust and is needed for cases wherever a trust relationship is created between two nodes without

previous interactions. It should conjointly receive this data second hand through the form of recommendations. This is often transitive trust; referred to as Indirect Trust. From this a belief level is often calculated on the routing behavior of this node it received from different nodes. A node could use a hybrid of those two approaches, like would be seen in reputation based trust management approaches [28].

5.3 Trust evaluation:

In ad hoc networks, the nodes process routing control messages and data messages.
In order to calculate the trust metric of each node, our algorithm use several types of messages, including:
Hello message, TC message and data messages routed through a node.
Upon receiving control messages or processing data messages our algorithm increment the trust value associated to each node of the network. And if a malicious behavior is detected our algorithm decrement the trust value.

To determine the weight associated with each type of message we use the Rank Order Centroïde method (ROC)

Step 1: Sort criteria in descending order of importance:

To sort criteria in descending order of importance we were based on two criteria:

- The resource consumption by processing these messages
- The benefit of nodes by exchanging these messages

The routing of data messages is the action which exhausts most resources as well as nodes have no profit to deliver the messages of other nodes.
The transmission of MPR messages consumes fewer resources than routing data messages as well as the nodes have no profit to deliver the messages to the other nodes
The transmission of Hello messages consumes fewer resources than routing data messages, but the nodes have to send periodically these messages to keep the connectivity with network nodes.
This is why we put the routed messages in the first rank and the TC messages in the second rank because nodes have no Benefit in sending these messages and HELLO messages at the 3rd rank because the nodes have to send these messages periodically to keep connectivity with network nodes.

Routed message > TC message > Hello message

Step 2: fill the matrix

	Routed msg	TC msg	Hello msg	Control
R1	1,00	0,00	0,00	1,00
R2	0,50	0,50	0,00	1,00
R3	0,33	0,33	0,33	1,00
Avg	0,61	0,28	0,11	1,00
				1,00

Step 3: provide weights

Weight	Routed msg	TC msg	Hello msg	Control
	0,611	0,28	0,11	1,00

The column control ensures that all weights are normalized (sum of weights = 1)
After this work, the formula becomes:

RTRST = 0.61 * ROUTEDmsg + 0.28 * TCmsg + 0.11 * HELLOmsg

Each node in the network calculate its neighbors trust and send it through the hello message.
After receiving the hello messages, each node can have a vision of other nodes trust by computing the confidence average of each node.

C. The overall performance computation:

After evaluating the trust metric, we can improve the security of our algorithm by adding this new metric in the computation of the overall performance of a node.
View the importance of trust metric, we will place it in the first rank when calculating the overall performance of a node:

Step 1: Sort criteria in descending order of importance:

RTRST > RAUT > RDENS > RRAM > RPRO > RHDD

Step 2: fill the matrix

	RTRST	RAUT	RDENS	RRAM	RPRO	RHDD	C
R1	1,00	0,00	0,00	0,00	0,00	0,00	1,0
R2	0,50	0,50	0,00	0,00	0,00	0,00	1,0
R3	0,33	0,33	0,33	0,00	0,00	0,00	1,0
R4	0,25	0,25	0,25	0,25	0,00	0,00	1,0
R5	0,2	0,2	0,2	0,2	0,2	0,00	1,0
R6	0,16	0,16	0,16	0,16	0,16	0,16	1,0
AV	0,41	0,24	0,16	0,10	0,06	0,03	1,0
							1,0

Step 3: provide weights

	RTRST	RAUT	RDENS	RRAM	RPRO	RHD	C
W	0.40	0.24	0.16	0.10	0.06	0.03	1

After this work, the formula becomes:

RPERF = 0,408*RTRST + 0,24 * RAUT + 0,16 * RDEN + 0,10 * RRAM + 0,06 * RPRO + 0,03 * RHD

6. PERFORMANCE BASED OLSR

6.1 PB-OLSR algorithm:

The MPR selection is the main step of OLSR. It has an impact on the performance of the network.
The objective of the Standard OLSR is to reduce the amount of broadcast traffic and minimize the overall network resource consumption, it is done by electing MPR nodes based on density and reachability criteria.

The objective of PB-OLSR is to:

- Reduce the impact of malicious nodes by including the trust metric in the selection criteria.
- Maximize the routing lifetime by avoiding nodes with poor resource profiles to be elected as MPR.
- Reduce the amount of broadcast traffic and minimize the overall network resource consumption by including the density metric in the selection criteria.

In order to do that each node calculates:

- Its neighbor trust
- Its own performance

Upon receiving a HELLO message, the node gets its trust metric. Then it can calculate its overall performance:

Operf (v) = perf (v) + trustValue (v)

After computing the overall performance the node sends it through the broadcasted Hello message.
When the other node receives Hello messages, it updates the related nodes' trust value and update its overall performance.
The algorithm allows each node to build all of its MPR is defined as follows:

x: the node performing the computation.
N: the set of neighboring nodes of node x
N2: all 2-hop neighbors, excluding:
- Nodes only accessible by members of N with willingness = WILL_NEVER
- The node x itself.
- All the neighbors of node x .symmetrical

MPR_Set: the set of all MPR for the node x.
OPerf (v): the overall performance of node v (where v is in N), which is the number of symmetric neighbors nodes of v,
Except of:
- All the members of N
- The node x itself

D (v) is the degree of node v (where v in N), which is the number of symmetric neighbors nodes of v,
Except of:
- All the members of N
- The node x itself

r (v) is the number of N2 nodes that are not yet covered by at least one node in the set MPR_Set, and are accessible via this node v

1. Calculate OPerf (v)
2.
   2.1. Add to MPR_Set the node v where v in N and v is the most performant and confident node
   2.2. Delete from N2 any node w currently covered with MPR_Set.
   2.3. If multiple choices are present, select the v that max (r)
   2.4. If multiple choices are present, select the v that max (D)

3. While N2! = {}
   3.1. Add to MPR_Set any node v of N which v is the only node to reach nodes in N2
   3.2. Delete from N2 any node w currently covered with MPR_Set.

4. The end of while.

7. SIMULATION RESULTS

To see the behavior of this approach and to measure the effect that will cause the implementation of our algorithm, we performed several simulations with variable number of nodes and different nodes velocity.
We used NS2 [29] as a network simulator with the following parameters:

TABLE I. NS2 PARAMETERS

Parameter	Value
Simulation area	1000 x 1000
Radio range	250 m
Number of nodes From	10 to 100 by step of 10
Velocity of nodes	From 0 m/s to 50 m/s by step of 5
Simulation time	300 s

We performed simulations with the standard OLSR and the PB-OLSR and we have recorded the average of MPR performance, the average delay, the average number of

collision occurred and the average number of non-routed packet.

7.1 Performance of MPR nodes based on the number of nodes:

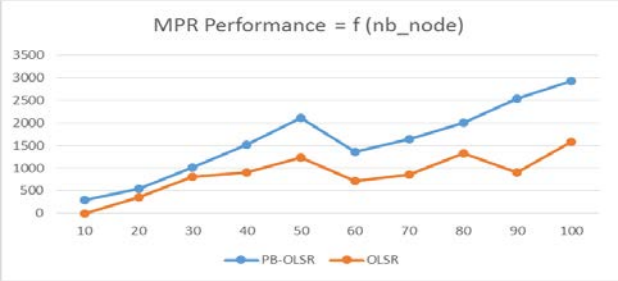

Fig. 1. Performance of MPR nodes = f (nb of nodes), V = 10 m/s

To approve the efficiency of our algorithm, we compared it with the standard OLSR protocol.
Collected results clearly show how the performance of the mpr node is enhanced when PB-OLSR is used against the Standard OLSR.
Which means that the MPR nodes in our algorithm are more powerful, densest and reliable, thing that will make them able to perform router tasks in the best conditions.

7.2 The average of non-routed packet under a selfishness network:

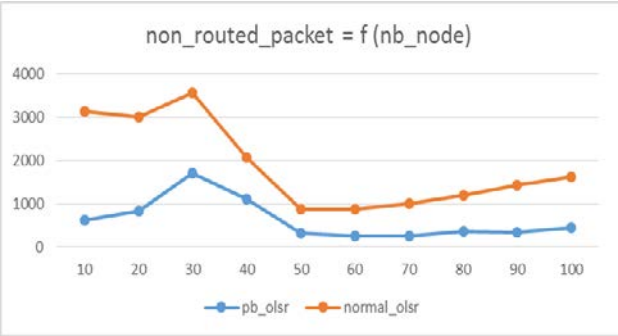

Fig. 2. Non-routed packet = f (nb of nodes), V = 10 m/s

To approve the efficiency of our algorithm, we compared it with the standard OLSR under a selfishness attack, and we measure the average number of non-routed packets.
We notice that in the standard OLSR the number of the non-routed packets is very important, it varies between 1622 and 3141, which threatens the proper functioning of the network.
but in our algorithm the number is less important, it varies between 442 and 607 thing that will improve the network performance.

7.3 The average end to end delay based on the number of nodes:

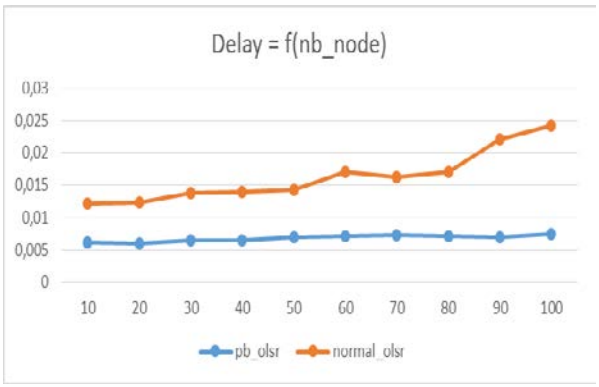

Fig. 3. Delay = f (nb of nodes), V = 10 m/s

By comparing the end to end delay of transmission between the standard olsr and PB-olsr, we notice that PB-olsr reduce significantly the delai of transmission, in the standard olsr the average of the end to end delay varies between 0.0060 and 0.016 while in PB-olsr it varies between 0.0059 and 0.0074

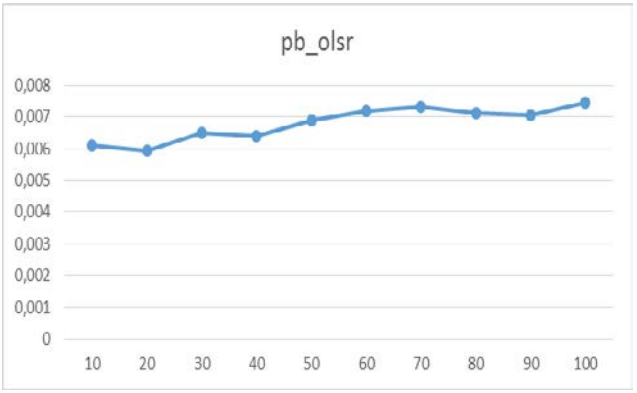

Fig. 4. Delay = f (nb of nodes), V = 10 m/s

This figure shows the same information in figure 4 but at different scale

7.4 The average number of collision based on the number of nodes:

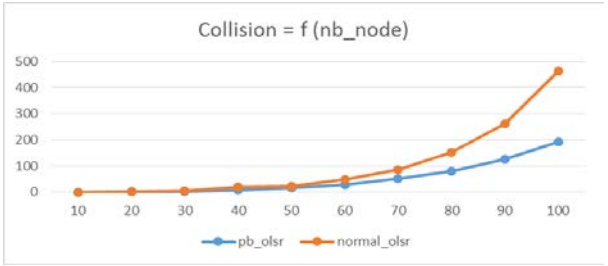

Fig. 5. Average Collision = f (nb of nodes), V = 10 m/s

Collision is the result of simultaneous data packet transmission between two or more network nodes, collisions disrupt the proper functioning of the network.
By comparing the average number of collision between the standard olsr and PB-olsr, we notice that PB-olsr has reduced significantly the number of collisions, in the standard olsr the average number of collision varies between 0 and 462.92 while in the PB-olsr it varies between 0 and 192.54

8. Conclusion

The OLSR protocol is a proactive routing protocol that use the concept of Multi-Point Relays (MPRs) to reduce the generated routing overhead. The main idea is to limit the number of retransmissions required for a node to flood a packet in the entire network
Certainly such a solution minimize the overall network resources consumption. However, OLSR overuses the resource of the MPRs nodes. In fact, resources is drained more quickly in MPRs nodes than in no-MPRs ones.
In this paper, we proposed an enhanced OLSR protocol named performance-based OLSR (PB-OLSR). The PB-OLSR allows the mobile nodes to create MPR sets with considering the performances and trusts of nodes.
The objective of PB-OLSR is to:
-Reduce the impact of malicious nodes by including the trust metric in the selection criteria.
-Maximize the routing lifetime by avoiding nodes with poor resource profiles to be elected as MPR.
-Reduce the amount of broadcast traffic and minimize the overall network resource consumption by including the density metric in the selection criteria.
Simulation results have confirmed the outperformance of PB-OLSR in comparison to the standard OLSR

References

[1] A. Boukerche, "Algorithms and Protocols for Wireless and Mobile Ad Hoc Networks", John Wiley & Sons Inc, Ottawa, Canada, 2009.

[2] A. Boukerche, B. Turgut, N. Aydin , M. Z. Ahmad , L. Bölöni and D.Turgut, "Routing protocols in ad hoc networks: A survey", Computer Networks,ELSEVIER, Vol.55, 2011, pp. 3032- 3080.

[3] P. Jacquet, P. Muhlethaler, T. Clausen, A. Laouiti, A. Qayyum and L. Viennot, "Optimized link state routing protocol for ad hoc networks", in IEEE INMIC, 2001

[4] T. CLAUSEN ET P. JACQUET. Optimized Link State Routing Protocol (OLSR).http://www.ietf.org/rfc/rfc3626.txt, 2003, RFC 3626

[5] N. LAKKI, A. OUACHA, A. HABBANI,1J.EL ABBADI "the integration ofthe speedof mobilityin the selection ofmpr to improve theqosin ad hoc networks." Journal of Theoretical and Applied Information Technology Vol. 36 No.2 2012

[6] N. Ghanem, "New energy saving mechanisms for mobile ad-hoc networks using OLSR" in the 2nd ACM International Workshop on Performance Evaluation of Wireless Ad Hoc, Sensor, and Ubiquitous Networks, 2005, pp. 273–274.

[7] Wardi , K. Hirata and Y. Higami , S. Kobayashi, " REOLSR: Residual Energy-Based OLSR Protocol in Mobile Ad Hoc Networks", IJMT Vol.1, 2011, pp.93-97.

[8] A. Benslimane, R. El Khoury, R. El Azouzi and S. Pierret, "Energy power-aware routing in OLSR protocol" in the First Mobile Computing and Wireless Communication International Conference, 2006, pp. 14–19.

[9] Z. Guo and B. Malakooti, "Energy aware proactive MANET routing with prediction on energy consumption", in the International Conference on Wireless Algorithms, Systems and Applications, 2007, pp. 287–293.

[10] S. Mahfoudh and P. Minet, "EOLSR: an energy efficient routing protocol in wireless ad hoc sensor networks", Journal of Interconnection Networks Vol.9 , 2008, pp. 389–408.

[11] F. De Rango, M. Fotino, and S. Marano, "EE-OLSR: Energy Efficient OLSR Routing Protocol for Mobile Ad Hoc Networks", in Military Communication Conference (MILCOM), 2008, pp. 1-7

[12] F.Lakrami and N. Elkamoun, " Energy and mobility in OLSR routing protocol",in Journal of Selected Areas in Telecommunications (JSAT), 2012.

[13] P. Michiardi, R. Molva, Core: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks, in: IFIP TC6/TC11 Sixth Joint Working Conference on Communications and Multimedia Security: Advanced Communications and Multimedia Security, 2002, pp. 107–121.

[14] L. Buttyan, J-P. Hubaux, Nuglets: a Virtual Currency to Stimulate Cooperation 1352 in Self-Organized Mobile Ad Hoc Networks, in: Technical Report DSC/2001/001, Swiss Federal Institute of Technology – Lausanne, Department of Communication Systems, 2001.

[15] A. Adnane, R.T. de Sousa Jr., C. Bidan, and L. Me. Autonomic trust reasoning enables misbehavior detection in OLSR. In SAC'08: Proceedings of the 2008 ACM symposium on Applied computing, pages 2006-2013, New York, NY, USA, 2008. ACM

[16] R. Abdellaoui and J.-M. Robert. SU-OLSR: A new solution to thwart attacks against the OLSR protocol. In 4th Conference on Security in Network Architectures and Information Systems (SAR-SSI), pages 239–245, Luchon, France, June 22–26, 2009

[17] Roy, B. (2005). An overview of MCDA techniques today: paradigms and challenges. In: Figueira, J., Greco, S. and Ehrgott, M. (eds) Multiple criteria decision analysis: state of the art surveys.

[18] http://www.ncsu.edu/nrli/decision-making/MCDA.php

[19] Butler J, Olson DL. Comparison of centroid and simulation approaches for selection sensitivity analysis. Journal of Multi-Criteria Decision Analysis 1999;8:146–61.

[20] Jia J, Fischer GW, Dyer JS. Attribute weighting method and decision quality in the presence of response error: a simulation study. Journal of Behavioral Decision Making 1998;11:85–105.

[21] StillwellWG, Seaver DA, EdwardsW. A comparison of weight approximation techniques in multiattribute utility

decision making. Organization Behavior and Human Decision Processes 1981;28:62–77.
[22] Sohail Abbas "A Survey of Reputation Based Schemes for MANET" PGNet 2010
[23] Yao Yu+, Lincong Zhang "A Secure Clustering Algorithm in Mobile Ad Hoc Networks" IPCSIT vol. 29 2012
[24] D. Gambetta, "Can we trust trust," Trust: Making and breaking cooperative relations, vol. 13, pp. 213–237, 2000.
[25] L. Capra. "Toward a Human Trust Model for Mobile Ad-hoc Network", Proc. 2nd UK-UbiNet Workshop, 5-7 May 2004, Cambridge University, Cambridge, UK.
[26] J. Li, R. Li, and J. Kato, "Future trust management framework for mobile ad hoc networks," Communications Magazine, IEEE, vol. 48, no. 4, pp. 108-114, 2008.
[27] A.A. Pirzada, and C. McDonald.: „Trust establishment in pure ad-hoc networks", Wireless Personal Communications, 2006, 37, pp. 39-168.
[28] Lidong Zhou, Zygmunt J.Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, vol.13, no.6, November/December 1999.
[29] Network Simulator NS2 http://www.isi.edu/nsnam/ns/

Mohamed DYABI Received the Master degree in networks and systems in 2010 from Faculty of Science and Technology HASSAN I University Settat-Morocco. Currently, he is a PhD Student in Computer Science. Ongoing research interests:Security in mobile ADHOC networks (MANETs) QoS in wireless networks Next Generation Networks

Prof. Abdelmajid HAJAMI PhD in informatics and telecommunications, Mohamed V-Souissi University Rabat-Morocco. 2011 Ex Trainer in Regional Centre in teaching and training Assistant professor at the Faculty of Science and Technology of Settat in Morocco Member of LAVETE Lab at Faculty of Science and Technology of Settat Research interests: Security and QoS in wireless networks Radio Access Networks Next Generation Networks ILE: informatics Learning Environments eLearning

Hakim ALLALI was born in Morocco on 1966. He received the Ph.D degree from Claude Bernard Lyon I University (France) in 1993 and the "Docteur d'Etat" degree from Hassan II-Mohamedia University, Casablanca (Morocco) in 1997. He is currently Professor at Faculty of Sciences and Technologies of Hassan 1st University of Settat (Morocco) and director of LAVETE Laboratory. He is executive manager and founder of IT Learning Campus. His research interests include technology enhanced learning, modeling, image processing, computer networking and GIS