SECURE ACTIVE ROUTING FOR PEER-TO-PEER NETWORKS

Hanafy M. Ali[(1)], Mohamed Z. Abdelmegid[(2)], and Mohamed M. Ali[(1)]

(1) Computers and Systems Engineering Dept. - Minia University.
(2) Computers and Systems Engineering Dept. - Al- Azhar University

(Received January 11, 2009 Accepted August 11, 2009).

This paper provides a single-node peer-to-peer (P2P) network architecture that integrates both active routing and P2P networking. The integrated architecture, as such is not full secure. Therefore, two security layers are added, one to compute the node reputation and the second to provide an authentication scheme. Such scheme may be either central or hierarchical. The integrated architecture gives us good results as the choice of the more trust bath is based on the reputation values of end nodes.

KEYWORDS: *- Active network-P2P network-security-routing – reputation.*

1. INTRODUCTION

In recent years, some ideas about deploying services and security at peer-to-peer (P2P) network to improve the performance and behavior of networked applications have been proposed. For this proposed, this paper introduces a new architecture of a secure active routing for P2P network. The proposed architecture depends on the active network. Active network technologies provide a programmable infrastructure for several network applications. Active nodes or active routers, which constitute active networks, are programmable and can be dynamically tailored to network administrators, applications, and even user's demands. Basically they process packets at a network layer, but they can apply application specific manipulation to packet payload if needed. Not only P2P applications, but all networked applications benefit from technologies that introduce some kind of intelligence into networks. If a network can offer application-dependent and tailored behaviors towards packets, including prioritized scheduling and intelligent routing, a higher QoS can be provided to users of overlying networked applications.

Most of current P2P services have security problems which play an obstacle to practical use [1-3]. Although P2P network must not only provide pseudonymity but also satisfy with strong authentication in case that a peer does business transaction with another one, most of current P2P services just adopt a weak authentication method using pseudonym and password or don't provide any authentication. The Groove Network provides public key based authentication mechanism [4-7]. However, this mechanism needs a central server that provides directory service for retrieving user's public key every time without having a legal force that can control and settle a dispute. A strong authentication mechanism and a reputation management for P2P system proposed without coping with server oriented paradigm, supporting pseudonymity and minimizing the cost of issuing certificate. Therefore, these authentication mechanisms

are not suitable to serious P2P commercial transactions which will happen in the near futures such as exchanging valuable information of knowledge, applying e-commerce, etc.

Therefore, P2P networks call for a purposed architecture which satisfy requirements ranging from pseudonymity to strong authentication based on certificate without particular server.

This paper is aimed at proposing a secure active routing P2P architecture which is based on two security layers, one to compute the node reputation and the second to provide an authentication scheme. Such scheme may be either central or hierarchical.

2.1 The Proposed Secure Active Routing Node Architecture

The active packet layer in the secure active routing for P2P architecture consists of four layers: p2p application layer, security tools layer, reputation computation layer and PLAN programs layer as shown in figure 1. In the proposed architecture, each node consists of five layers: Link layer (Ethernet), node operating system layer, P2P networking layer, active extension layer and active packet layer as shown in figure 1. The P2P application layer implements P2P applications and services. The active packet layer accommodates P2P applications, security tools, reputation computation and PLAN programs. The active extension layer includes the PLAN interpreter and routing extension. The P2P network layer implements network connection between nodes. The link layer implements TCP and UDP protocols. The PLAN interpreter is written by Ocaml language. The active packet and extension layers make the PLAN daemon running. Every node must have the PLAN daemon running. The source node sends a packet to a destination node for remote evaluation. The packet traverses all intermediate nodes without evaluation, regardless of whether it is written by PLAN code or not. The proposed secure active routing for P2P architecture implementation runs in user-space on Linux (operating system OS) machines and uses Ethernet as its main underlying link layer, as well as UDP as a pseudo-link layer. The implementation is written in Ocaml language.

The security system takes place in three phases. First, the reputation algorithm is used to know the most trust path which is based on the reputation values and distance metrics. Secondly, the application that injects PLAN program into the network must authenticate itself with the node on which secure access is requested. This is done by an exchange of messages (protocols) which allows both parties to derive a shared secret. Third, after the authentication protocol has taken place, the user uses the shared secret to sign a chunk (a piece of code) to be executed on the secured node. Before evaluating the chunk, the node verifies the signature as that of the purported identity of the code.

Resident data remains on the router after terminating the PLAN program. Resident data is stored in a table on the router that is indexed by a string which names the data, and session key. This key serves to differentiate data stored at different instances of the same PLAN applications.

One hazard of resident data is that PLAN program may leave large chunks of data on a router, consuming memory even after the termination of the PLAN program.

To combat this problem, each piece of resident data has a timeout associated with it. This timeout is set by the user when the data is created.

2.2 Active Packet

Active packets carry software programs consisting of both data and code that take place on classical packet headers and payloads. Basic data transport can be implemented with a code that takes the destination address part of its data, looks up the next hop in a routing table, and then forwards the entire packet to the next hop. At the destination, the code delivers the payload part of the data. For pragmatic reasons, our implementations do use some traditional headers and payloads. For example, to tunnel an active packet through the IP Internet between active routers, the packet is encapsulated in a standard UDP packet, and transported over an Ethernet which requires the use of standard headers and trailers.

The code part of an active packet is able to execute the function of a packet header with much more flexibility, since it can interact with the router environment in a more complex and customizable fashion than the simple routing table lookup. The data in the active packet is a customizable structure that can be easily manipulated by the program. The programming language used by this layer is PLAN. The PLAN programs are composed of three distinct parts: the code, the entry point, and the bindings; the latter two are referred to collectively as the invocation. The code consists of a series of definitions that bind variables to either functions, simple values (i.e. integers, strings, etc.), or exceptions. The invocation defines the function call (i.e., function name entry point and actual parameters). The parameters are called the bindings to be evaluated at the evaluation destination (or evalDest), which is stored in the packet. To resolve variables mentioned in the invocation, the set of all definitions in the code part and the core service functions serve as the legal environment for the call.

3. REPUTATION ALGORITHMS

A reputation is an expectation about an agent's behavior based on information about or observations of its past behavior [8-18]. However, distributed reputation algorithm is used to calculate the global reputation [14] for use in the design the active p2p networks.

The global reputation was calculated using the following formula:

$$R_i = \sum_{j \in s} \left[\frac{w_j}{\sum_{j \in s} w_j} t_{ji} \right] = \frac{\sum_{j \in s} w_j t_{ji}}{\sum_{j \in s} w_j} \qquad \text{Eq. (1)}$$

Where:-

R_i: is the global reputation of peer i,

S : is the set of peers with whom peer i has conducted transactions,

t_{ji} : is the local trust score of peer i rated by peer j.

w_j:- is the aggregation weight of $t_{ji.}$

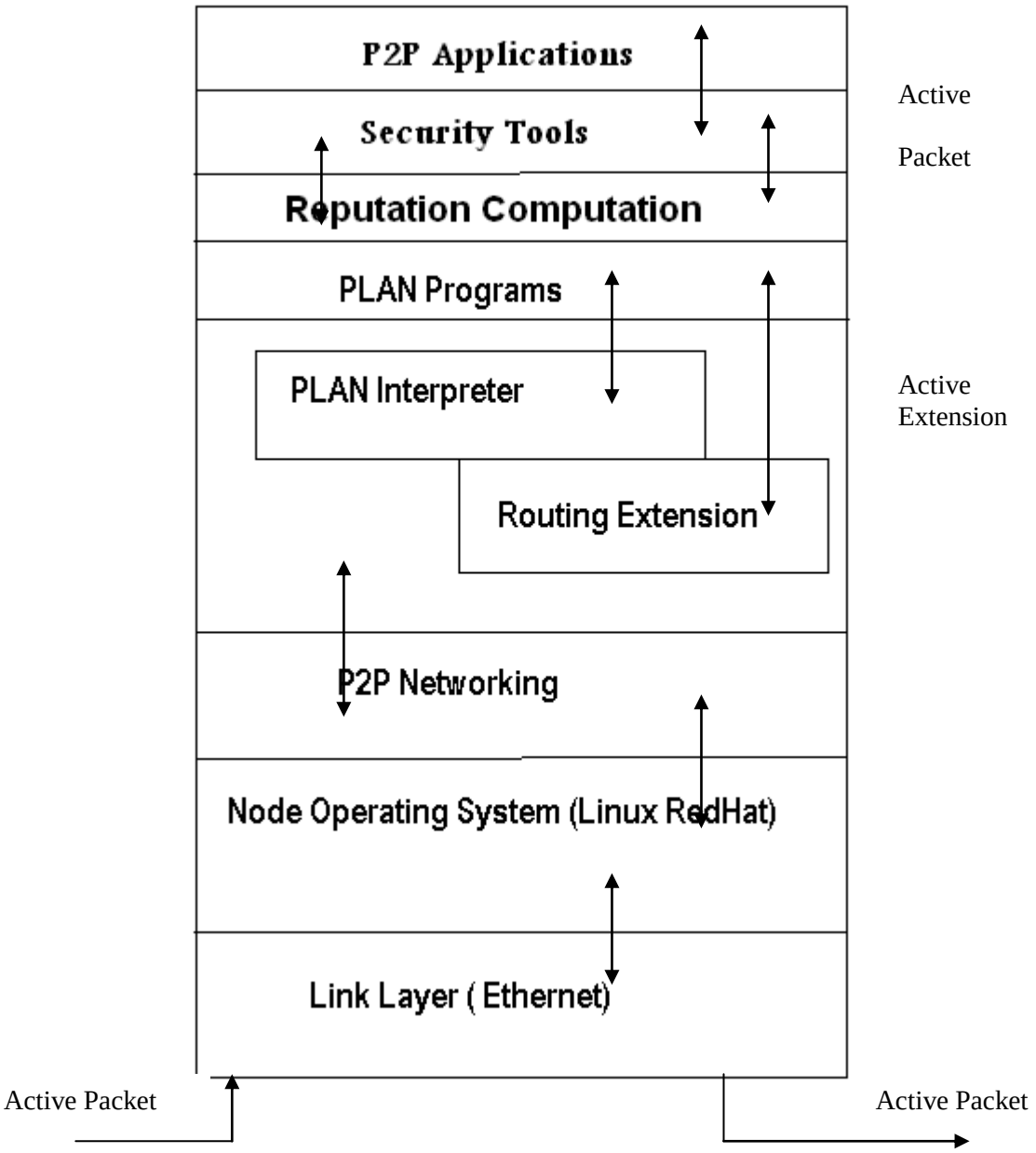


Figure 1: Proposed secure active routing node architecture

The global aggregation process runs multiple iterations until each R_i converges to a stable global reputation rating for peer i.

A router is a network node specialized in packet switching and processing. It determines the next node to which a packet will be forwarded in order to reach the destination.

The RIP (Routing Information Protocol) style is used to dynamically determine the routing tables of the PLAN node it can used the static routing table. The RIP discovers its neighbors and learns their network addresses, measures the delay to each of its neighbors, computes the shortest path to every other router and sends this packet to all other routers. The shortest path depends on the distance metric. In the proposed active secure routing, calculating of the distance metric depends on the distance and reputation value. The reputation value is calculated by equation 1.

The scout plan program is used to determine the best routing path based on the modified distance metric

$$D_{mi} = D_i + a/Rep_i \qquad \text{Eq. (2)}$$

Where:-

D_{mi} : the modified distance metric of peer i

D_i : the distance metric of peer i

a : a parameter

Rep_i : the reputation value of peer i

The network topology in figure 2 is implemented using the proposed active secure routing architecture. The system is investigated for different malicious nodes. Figure 3 indicates the good path (No. of malicious nodes/No. of trust nodes in the routing path) against the number of malicious nodes. The proposed routing architecture gives 100% good path for malicious nodes up to 50%. It is worthy to mention that the routing architecture gives good path for more than 50% malicious nodes on increasing the number of nodes above 5 nodes.

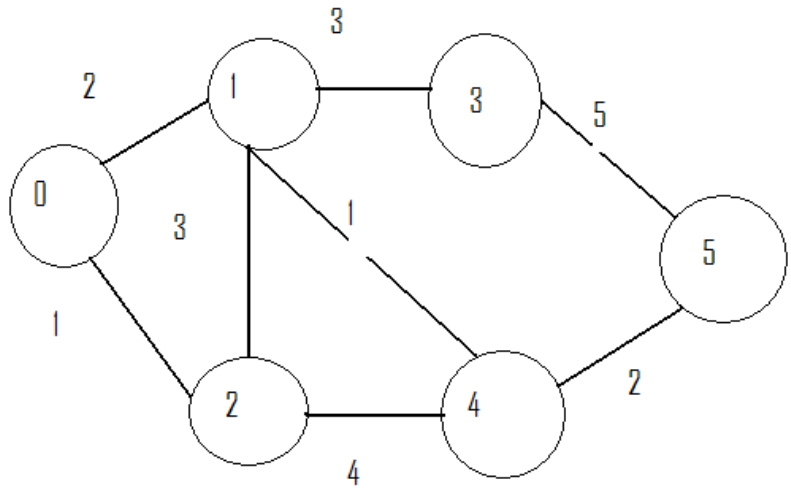


Figure 2:- Network topology with alternate paths

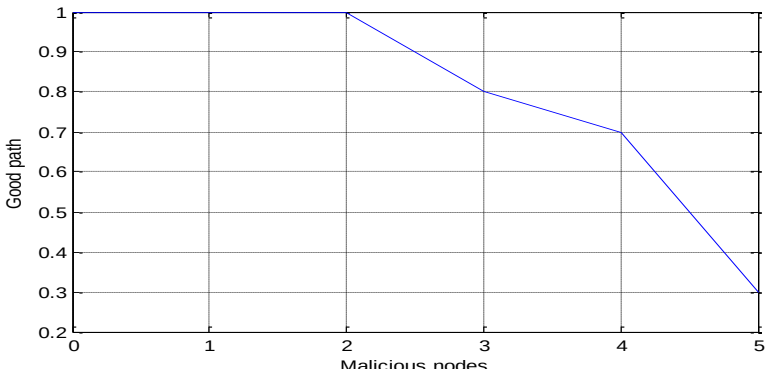


Figure 3: The relation between malicious node and good path

4. IMPLEMENTATION

A Unicast function is used to deliver data from source to destination. The arguments for the unicast function include the open port and deliver functions. The open port function attempts to create a connection between the invoking host and server application as shown in figure 4. If successful, the function returns a port naming that connection. The deliver function injects the data though the specific port; converts the data to a string, and structurally marshalls the data before sending across the connection. Then, the host application listens on the specified port through the connection, and then prints any values received through the port.

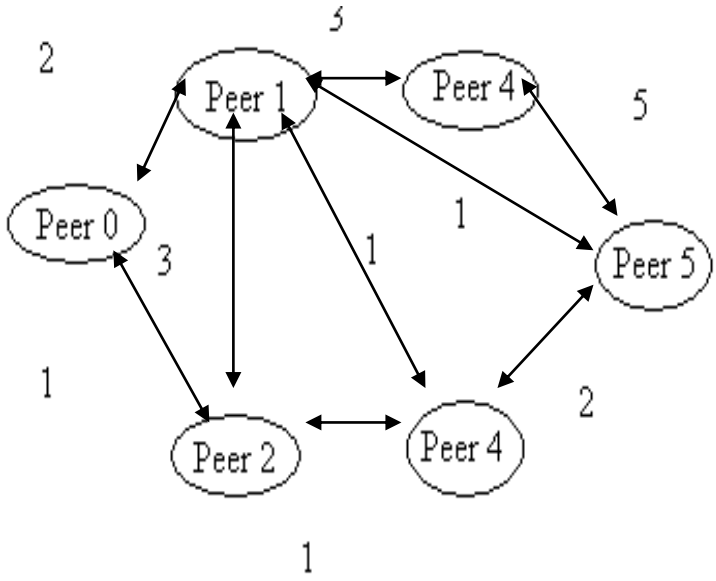
Unicast function is used to send data from peer 0 to peer 5 in a network shown in figure 5.a. In this application, peer 5 acts as server which listens on the specified port for connection and prints any values received through this port. The unicast function is enforced dynamically by the interpreter. The RB (Resource Bounded) carried by each packet decreases each time the packet passes a peer through the connection from the source to the destination.

```
Fun unicast(num)=
  try
    let val m = openPort(num)  % open port function
        val h = "Pay for Ali $"% h is string value
        val i = 1000           % I is integer value
      in
       (deliver(m,h); deliver(m,i); deliver(m,m); % deliver
function
        closePort(m))                              % close the
port
    end
     handle OpenFailed =>
    (print("No server listening on host ");
     print(" on port ");
     print(num))
```

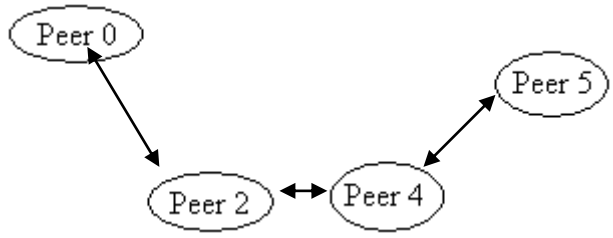
Figure 4: Uni-cast function

The deliver application is implemented using the secure active routing architecture and the traditional (Passive) architecture which is based on RIP protocol, respectively. Table 1 shows the trust score and weight values used in application. The packet in the secure active routing architecture takes path 0-2-4-5. This path is more secure than the other paths, as shown in figure 5.b because the reputation value is the highest as calculated in table 2. The packet in the passive architecture takes path 0-1-5. This path is the shortest path than others, as shown in figure 5.c. This is an advantage when compared with the path 0-2-4-5 of figure 5.b. However, the path 0-1-5 is less secure than the path 0-2-4-5.

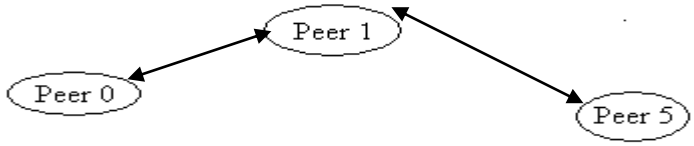
The active extension layer in the proposed architecture of the intermediate nodes route the uni-cast function based on the routing algorithm. The active packet layer in the destination node evaluates the uni-cast function.



a. Investigated network



b. Active secure routing path



c. The routing path based RIP protocol

Figure 5 Routing paths in uni-cast application

Table 1:- Trust Score and weight values

Node	The aggregation weight	Node	Trust Score
W_1	0.1	t_{01}	0.2
W_2	0.9	t_{02}	0.8
W_3	0.4	t_{03}	0.2
W_4	0.9	t_{04}	0.8
W_5	0.8	t_{05}	0.8

Figure 6 shows the relation between the bandwidth and the number of hops for the proposed and passive architecture. It is cleary that the proposed architecture decreases the bandwidth to 40% against 90% for traditional (passive) network. Therefore, the proposed architecture improves the bandwidth by (0.9-0.4)/0.9 = 55%.

It is worthy to mention that the proposed architecture opens and closes specific port for data injection which is not possible for passive network.

Table 2:- Final routing paths

paths	Reputation
0-1-3-5	(0.1*0.2+0.4*0.2+0.8*0.8)/(0.1+0.4+0.8)=0.58
0-1-4-5	(0.1*0.2+0.9*0.8+0.8*0.8)/(0.1+0.9+0.8)=0.76
0-2-1-3-5	(0.9*0.8+0.1*0.2+0.4*0.2+0.8*0.8)/(0.9+0.1+0.5+0.8)=0.63
0-2-1-4-5	(0.9*0.8+0.1*0.2+0.9*0.8+0.8*0.8)/(0.9+0.1+0.9+0.8)=0.77
0-2-4-5	(0.9*0.8+0.9*0.8+0.8*0.8)/(0.9+0.9+0.8)=0.8
0-1-5	(0.1*0.2+0.8*0.8)/(0.1+0.8)=0.7

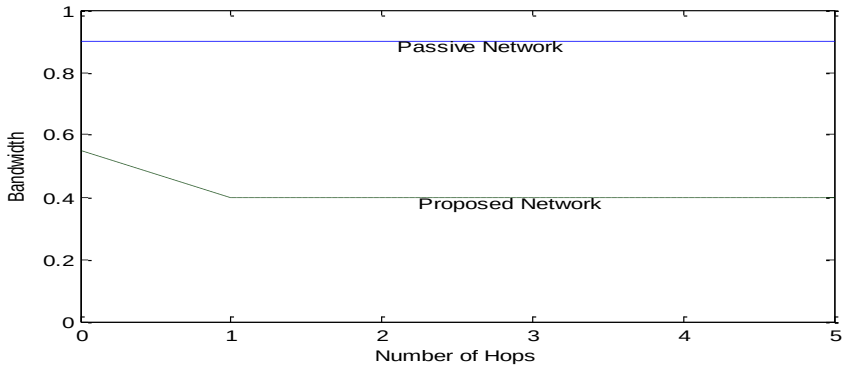


Figure 6 Bandwidth versus number of hops

5. CONCLUSIONS

The architecture integrating active router and P2P networking is fully secure. Two security layers are added to enhance the security; one to compute the node reputation and the second to provide an authentication scheme. Such scheme may be either central or hierarchical.

The proposed enhanced-security integrated architecture of active P2P networks avoids the drawbacks of the passive network which include impossibility of calculation, data injection in specific ports, closing or opening of ports and protection from hackers. The proposed secure active routing architecture gives 100% good path for malicious nodes up to 50% for a 5-node network. It gives good path for more than 50% malicious nodes on increasing the number of nodes above 5 nodes.

The deliver application is investigated as being considered a unicast communication case study of both the proposed active P2P architecture and the proposed secure active routing architecture for P2Pnetworks. The packet in the proposed active P2P network takes the shortest path, while it takes the most secure path in the secure active routing architecture.

REFERENCES

1- S. Marti and H. G. Molina, “Taxonomy of Trust: Categorizing P2P reputation systems”, IEEE Computer Networks, Vol. 50, pp: 472-484, 2006.
2- Z. Despotovic and K. Aberer, “P2P estimation vs. social networks”, IEEE Computer Networks, Vol. 50, pp: 485-500, 2006.
3- M. Cupta, M. H. Ammar and M. Ahamad, “Trade-offs between reliability and overheads in peer-to-peer reputation tracking” IEEE Computer Networks, Vol. 50, pp: 501-522, 2006.
4- R. Sherwood, S. Lee and B. Bhattacharjee, “Cooperative Peer Groups in NICE”, IEEE Computer Networks, Vol. 50, pp: 523-544, 2006.
5- L. Mekouar, Y. Iraqi and R. Bootoba, “Peer-to-Peer’s most wanted: Malicious Peers”, IEEE Computer Networks, Vol. 50, pp: 545-562, 2006.
6- T. G. Papaioannou and G. D. Stamoulis,” Reputation-based Policies that provide the right incentives in peer-to-peer environments”, IEEE Computer Networks, Vol. 50, pp: 563-578, 2006.
7- V. Pathak and L. Iftode, “Byzantine fault tolerant public key authentication in peer-to-peer systems”, IEEE Computer
8- K. Aberer and Z. Despotovic, “Managing Trust in a Peer-2-Peer Information System,” *Tenth International Conf. on Information and Knowledge Management,* New York, 2001.
9- S. Buchegger and J.-Y. L. Boudec, “A Robust Reputation System for P2P and Mobile Adhoc Networks”, *Second Workshop on Economics of P2P Systems*, Boston, June 2004.
10- D. Dutta, A. Goel, R. Govindan, and H. Zhang, “the Design of a Distributed Rating Scheme for Peer-to-Peer Systems,” *First Workshop on Economic Issues in P2P Systems,* Berkeley, June 2003.

11- S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks", *ACM WWW'03,* Budapest, Hungary, May 2003.
12- S. Marti and H. Garcia-Molina, "Limited Reputation Sharing in P2P Systems", *Proc. of the 5th ACM conference on Electronic Commerce,* New York, May 2004.
13- A. Singh and L. Liu, "TrustMe: Anonymous Management of Trust Relationships in Decentralized P2P Systems", *IEEE Intl. Conf. on Peer-to-Peer Computing*, Sep. 2003.
14- S. Song, K. Hwang, R Zhou, and Y. K. Kwok, "Trusted P2P Transactions with Fuzzy Reputation Aggregation", *IEEE Internet Computing*, pp.18-28, Nov/Dec. 2005.
15- M. Srivatsa, L. Xiong, and L. Liu, "Trustguard: Countering Vulnerabilities in Reputation Management for Decentralized Overlay Networks", *Proc. of the 14th International World Wide Web Conference,* pp: 422–431, 2005.
16- L. Xiong and L. Liu, "PeerTrust: Supporting Reputation-based Trust for Peer-to-Peer Electronic Communities", *IEEE Trans. Knowledge and Data Engineering,* Vol.16, No.7, pp. 843-857, 2004.
17- B. Yang, T.Condie, S. Kamvar and H. Garcia-Molina, "Non-Cooperation in Competitive P2P Networks", *Proceedings of the 25th IEEE International Conference on Distributed Computing Systems* (ICSCS'05), Columbus, Ohio, 2005.
18- S. Kamvar, M. Schlosser, and H. Garcia-Molina, "The Eigentrust Algorithm for Reputation Management in P2P Networks", *ACM WWW'03,* Budapest, Hungary, May 2003.

المسار الأيجابى الأمن لشبكات الند للند

هذا البحث يقدم تكوين جديد لنهاية طرفية لشبكات الند للند وهذة النهاية الطرفية تجمع بين المسار الايجابى وشبكة الند للند. هذا التكوين الجديد يحتاج الى زيادة درجة الأمان ولذلك طبقتين تم أضافتهم الى التكوين وهما طبقة مبنية على السمعة للنهاية الطرفية والطبقة الأخرى مبنية على درجة الثقة للنهاية الطرفية. التركيب الجديد للنهاية الطرفية يقدم نتائج جيدة فى أختيار المسار الأمن للحزمة الشبكية وهذا المسار مبنى على درجة السمعة للنهايات الطرفية.