ACTIVE NETWORK SECURITY BASED RSA ALGORITHM

Ahmed Freidoon Fadhil
Civil Engineering Department
University Of Kirkuk

Wisam haitham abbood Computer and Software Engineering Department
University Of Al- Mustansiriya

ABSTRACT

The difficulty of building a secure network is due to the changing nature of the enterprise coupled with the increasing sophistication of the hacker threat, both from inside and outside of the network. Active networks enable individual user or groups of users to inject customized programs into the nodes of the network.

The proposed system depends on the basic concepts (authentication and authorization) and uses RSA algorithm to add additional level of security. The proposed system also depends on active packet architecture, the packet will represented in the active node as input, and when the packet is retransmitted to another active node it carries information about each node it visits. The result of execution the packet will display in the first node where the packet started.

الخلاصة

إن الصعوبة في بناء شبكة آمنة للحاسبات ترجع إلى الطبيعة المتغيرة لمشاريع الشبكة إضافة إلى المهارة المتزايدة لقراصنة المعلومات سواء من داخل الشبكة أو من خارجها. الشبكات الفعالة (Active Network) تسمح لمستخدم واحد او مجموعة من المستخدمين ليدخل برامج مُعَدة حسب الطلب الى حاسبات الشبكة.

ان النظام المقترح يعتمد على المفاهيم الرئيسية (التوثيق، التخويل) و يستخدم خوارزمية التشفير (RSA) لزيادة امن النظام. يعتمد النظام المقترح ايضاً على معمارية الحزمة النشيطة (Active packet)، ان الحزمة (Packet) ستتمثل في الحاسبة الفعالة كمدخل, وعندما يتم نقل الحزمة الى حاسبة فعالة اخرى فانها سوف تحمل معلومات عن كل حاسبة زارتها. وان نتيجة تنفيذ الحزمة سوف يعرض في اول حاسبة كانت الحزمة بدأت فيها.

KEY WORDS

Active network, Security, Authentication, Authorization, RSA .

INTRODUCTION

Computer networks are becoming fundamental to the functioning of modern organizations. As the dependency on networks increases, the need to control networked resources becomes increasingly critical. At the same time, networks are becoming ever more valuable in terms of their function, the resources they offer, and the information they contain. In this way, they become not only more valuable to an organization itself but they also become an attractive target for hostile parties (both in and outside of an organization) (Gert D. L. 2005).

In the past decade, a wide variety of security mechanisms have been developed, aimed at safeguarding the logical assets of an organization: firewall technologies, encryption and

cryptographic authentication, biometrics and the like. These measures have one common factor in that they attempt to prevent unauthorized access to resources they could be likened to the locks and secure doors used in physical security (Gert D. L. 2005).

When performing security tasks, security professionals tray to protect their environments as effectively as possible. These actions can also be described as protecting confidentiality, integrity, and availability (CIA).

CIA stands for:-

- Confidentiality:- ensure that no data is disclosed intentionally or unintentionally.
- Integrity:- make sure that no data is modified by unauthorized person, that no unauthorized changes are made by unauthorized person.
- Availability:- provide reliable and timely access to data and resources.

There is an idea (active network) that gives the user the ability to program the network (Psounis K. 1999).

ACTIVE NETWORK

The concept of active networking emerged from discussions within Defence Advanced Research Projects Agency (DARPA) research community in 1995 on the future direction of networking systems (Tennenhouse D. L. 1997).

Active Networks break with tradition by allowing the network to perform customized computations on the user data. For example, a user of an active network could send a customized compression program to a node within the network (e.g., a router) and request that the node execute that program when processing their packets. These networks are "active" in two ways:

- Routers and switches within the network actively process, i.e., perform computations on, the user data flowing through them.

- Individual authorized users and/or administrators can inject customized programs into the network, thereby tailoring the node processing to be user and/or application specific (Tennenhouse D. L. 2002).

There are three principal advantages to basing the network architecture (on the exchange of active programs, rather than static packets):

- Exchanging code provides a basis for dynamically adaptive protocols, enabling richer interactions than the exchange of fixed data formats.

- Active packet provides a means of implementing fine grained application-specific functions at strategic points within the network.

- The programming abstraction provides a powerful platform for user-driven customization of the infrastructure, allowing new services to be deployed at a faster pace than can be sustained by vendor driven standardization processes (Tennenhouse D. L. 2002).

So, active network would enable a range of applications that leveraged computation within the network, and it would accelerate the pace of innovation by decoupling services from the underlying infrastructure (Whetherall D. 1999).

ACTIVE NETWORK ARCHITECTURES

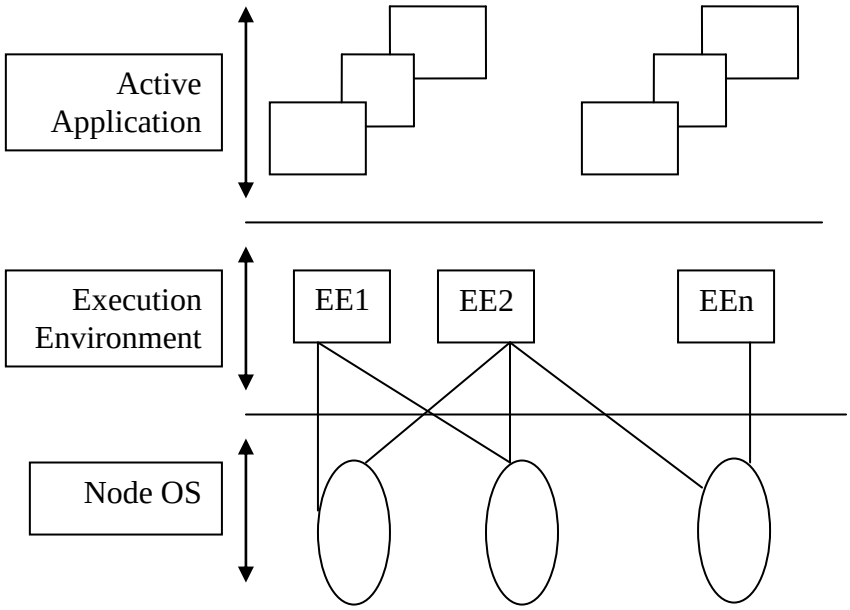


Fig. (1): Active Network Architecture

The architectures are classified based on their approach toward the realization of active networking. **Figure 1** shows the high level AN node (Active Network Node) architecture. Each AN node runs an operating system (Node OS) and one or more execution environments (EE). When a packet arrives at a node, it will be first handled by the Node OS. Node OS verifies and identifies the content of that packet. If the packet does not require further process, it is then simply forwarded to the next node. If further process is needed, the packet is passed to the EE. The further process in the EE may include running an active application or simply store the data brought by the packet.
There are currently three architectures in implementing active network:
Active packets, active nodes and hybrid approaches. Most of the early active networks architectures follow "the active packet" approach. This scheme is fundamentally characterized by the fact that the code is carried inside the packet. The nodes are also active in a sense that they allow computation up to the application layer (Clavert K. L. 1999).

❖ Active Packet Approach

In active packet the code is carried by the packets. The code is either to be executed on the data of the same packet that carries the code or to be executed in order to change the state or the behavior of the node (Bhattacharjee S. 1999).

Service CODE	DATA

Fig. (2): Active Packet Approach Representation

❖ **Active Node Approach**

In this approach, the packets do not carry the actual code or program. Instead, the packet carries some identifiers or references to functions reside in the active nodes. The packet, nevertheless, is considered active in a sense that they decide which functions are going to be executed on their data, and they provide the parameters for these functions (Jean-Patrick G. 2003).

Service ID.	DATA

Fig. (3): Active Node Approach Representation

❖ **Hybrid Approach**

Active packets can carry code efficiently only when the code is relatively simple and restricted. On the other hand, active nodes can efficiently provide any code given that the code is predefined. In the hybrid architecture, active packets carry actual code and other more complex code resides in active nodes. Hybrid architecture makes possible to use more complex programs and be flexible enough to program command or parameters in data packets (Eva H. 2001).

SECURITY ISSUES IN ACTIVE NETWORKS

To provide security in the active network, we need two basic services: authentication and authorization.

Authentication is the core of many current security mechanisms, it encompasses the technologies used to identify and verify the authenticity of users, network components and processes. This ranges from simple password based schemes through to biometric and cryptographic mechanisms. The ultimate goal is to uniquely associate an entity external to a system with an identity stored inside the system. In most systems, this is done by requesting some identifying information from a client, for example a password, biometric reading or response to some challenge. This information is then verified against information held inside the system. When the identifier and stored information are match, the user is authenticated; otherwise the user is denied (Ravi S. 1996). **Figure 4** provides a graphical overview of the authentication method.

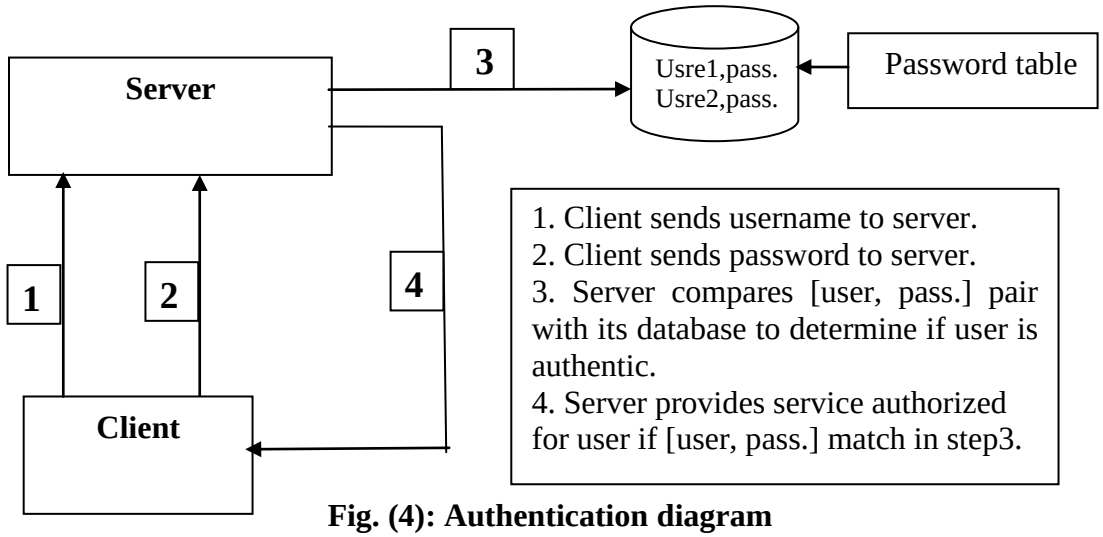
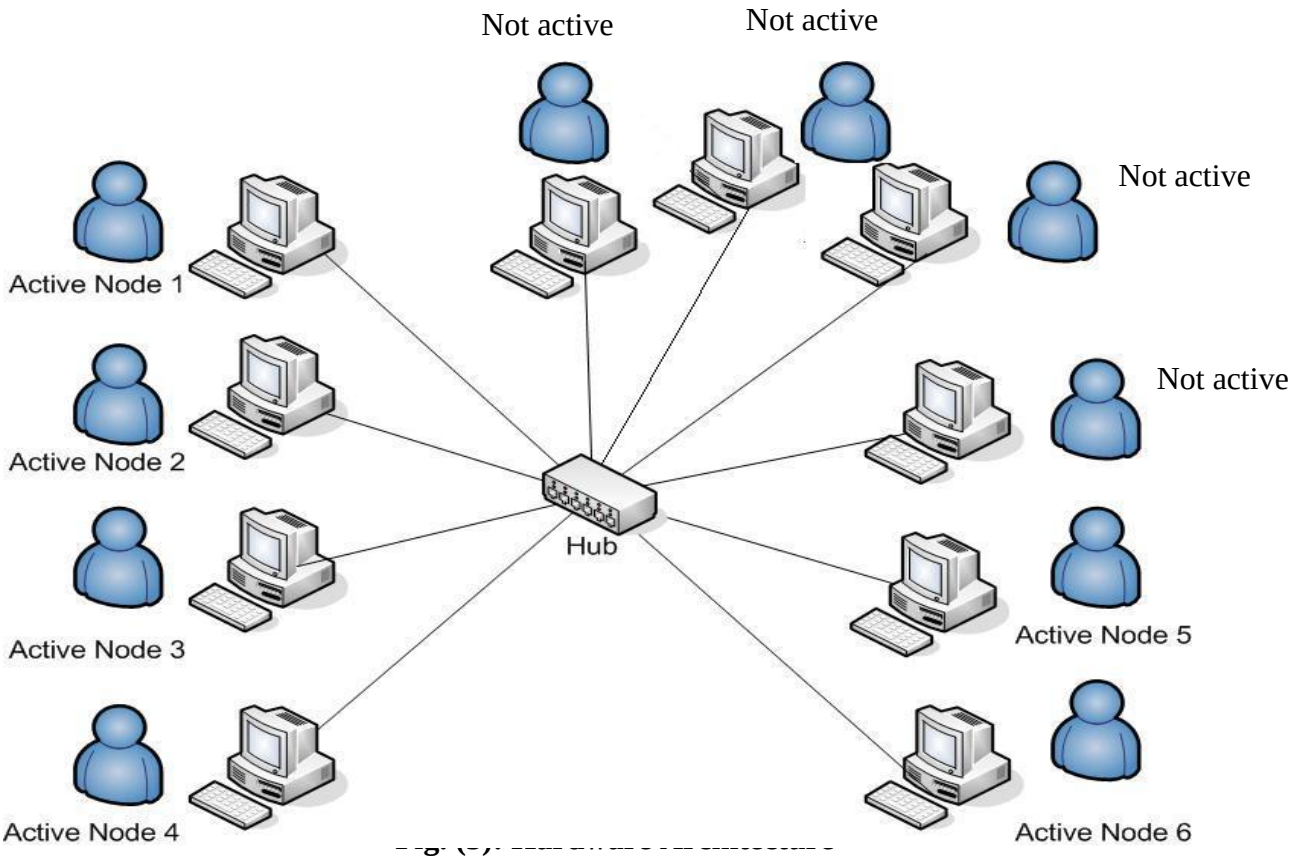


Fig. (4): Authentication diagram

In an active network, authorization to perform some requested access or action would be the overwhelming security concern. The authorization may take the form of control of access to objects or functionality, control of exposure of data, or control of resource usage. Authentication and authorization are somewhat tightly-coupled mechanisms; authorization systems depend on secure authentication systems to ensure that users are who they claim to be and thus prevent unauthorized users from gaining access to secured resources (Laat 2000).
The proposed system depends on (authentication and authorization) and used RSA (encryption-decryption) algorithm to add additional level of security.

PROPOSAL SYSTEM

The proposed system was built using the hardware architectures that show in **Fig. 5**.



THE DESIGN PROCESS

The proposed system contains two parts, the first part is security and the second part is active network part, installed in active PC for the purpose of security by examining the received packet from inside and outside.

The proposed program installed on PCs waiting to be active (in the work the number of active PCs is 6), the active node is the PC that

- Have a program permits to make the packet passing inside it.
- The ability to make secure execution on packet.
- The authentication and authorization role are defined inside it.

- The encryption and decryption algorithm done inside it.
- When active node is busy it will search for another active node which is Idle to continue processing.

Note that all IP (Internet Protocol) addresses of active nodes are defined in packet and the active node will be busy when there is fault in PC or normal termination. The proposed system was written in Microsoft Visual Basic version 6 and uses window manner in its work. As well as it uses the database to store the information like username, password, job, and the information about authorization. And it has API (Application Program Interface) tools (An API is simply a set of functions that can be used to work with a component, application, or operating system), these functions that can be called from any application running in Windows. At run time, a function is dynamically linked into the application that calls it.

❖ **Security Part**

This part is used for securing the active node. It will exam the received packet from inside and from outside. This part is relay on the concepts authentication, authorization and encryption.

Now the first case depends on authentication and authorization rule, the authentication rule is as follows:

- Username
- Password
- Job
- E-mail

If the username and password is entered three times incorrect then the Program terminates.

The authorization rule is as follows:

- Permit the user to use the active PC
- Permit the user to present the result
- Permit the user to use the active PC and present the result

The information about authentication and authorization is verified against information reside inside the system, the packet is authenticated if the identifier and stored information is match, otherwise the packet is denied. Incase of authenticated packet, active node will make a secure execution on it. When packet move from one active node to another, during processing, it carry's information about each node it visit.

Second case, this part also depends on encryption by using RSA algorithm to increase the security. The RSA algorithm is explained as follows:

1. Generate two random prime numbers p and q.
2. Multiply p and q together to generate N.
3. Choose another number e which must be relatively prime to (p-1) (q-1).
4. Calculate the value of ciphertext as $C=M^e \pmod N$.
5. Find d such that: $e*d=1 \pmod{(p-1)(q-1)}$.
6. Calculate the value of plaintext message as $M= C^d \pmod N$.

Where

M: plaintext message.
C: ciphertext message.
Public key: (e, N).
Private key: (d, N).
Now if we choose p=11, q=3 then
N=33.
(p-1) (q-1) =20.
Let Z= (p-1) (q-1).
Suitable value for e =3, since 3 and 20 have no common factors.
With these choices, d can be found by solving the equation:
3d=1 (mod 20).
Which yield d = 7.
The ciphertext, C, for a plaintext message, M, is given by
$C=M^3 \pmod{33}$.
The ciphertext is decrypted by the receiver by making use of rule:
$M=C^7 \pmod{33}$.

❖ Active Network Part

This part is divided into two subparts, client part and server part. After the active node receives the packet, the server part will begin working on it, in case of transmitting the packet to another active node to continue the processing, the server should changed to the client part and the server part of the new active node will receive the packet and work on it.

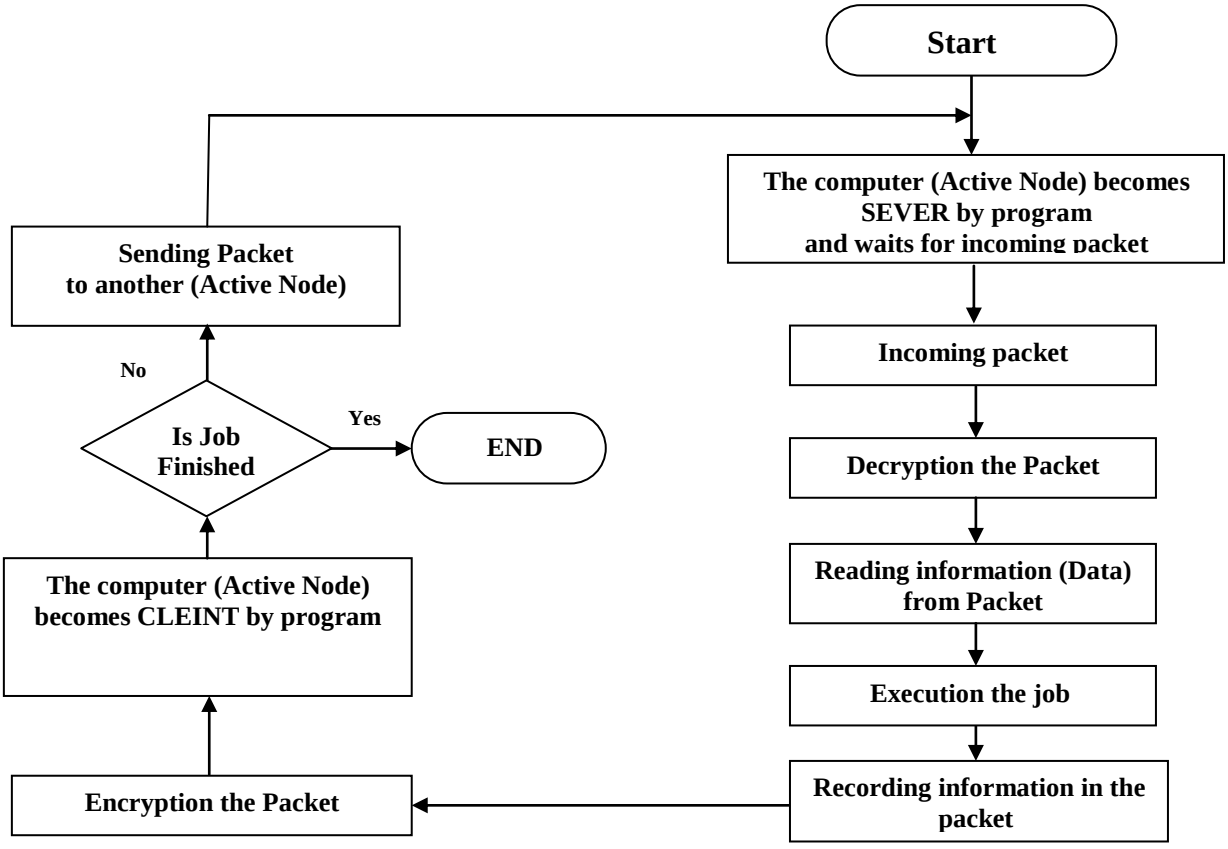


Fig. (6) : The lifecycle of Packet in active node

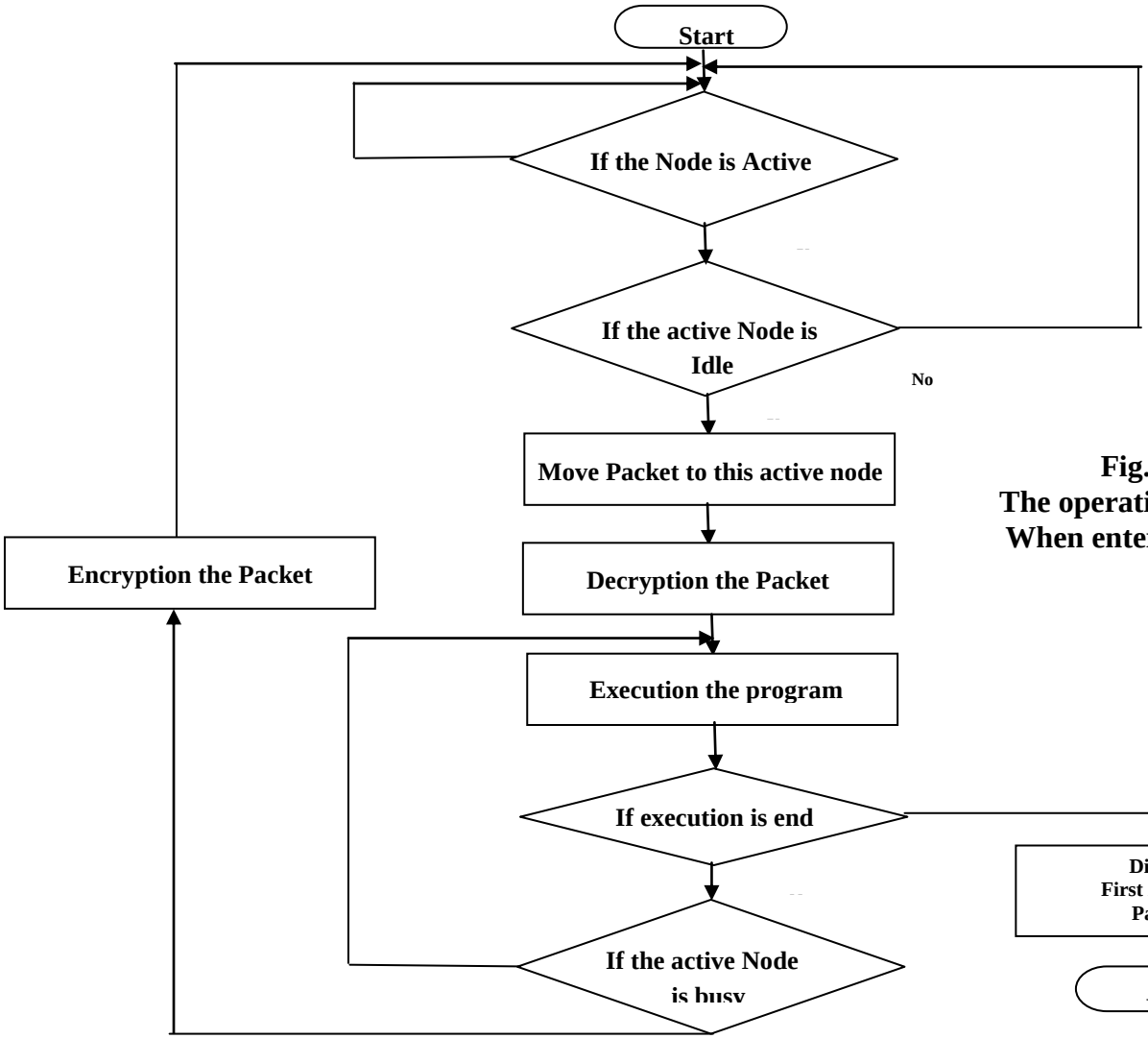


Fig. (7) :
The operation on Packet When enter active node

*** THE SOFTWARE PROCESS**

The Program is performed as follows:-

Step 1:- initially install the program in computer 1.

Step 2:- the program ask about username and password.

Step 3:- input IP address for all active nodes.

Step 4:- input information and suitability for users that use active nodes.

Step 5:- then install the program on all PC's we want them to be active.

Step 6:- input the job, for our example (Loop count) as shown in **Fig. 8**.

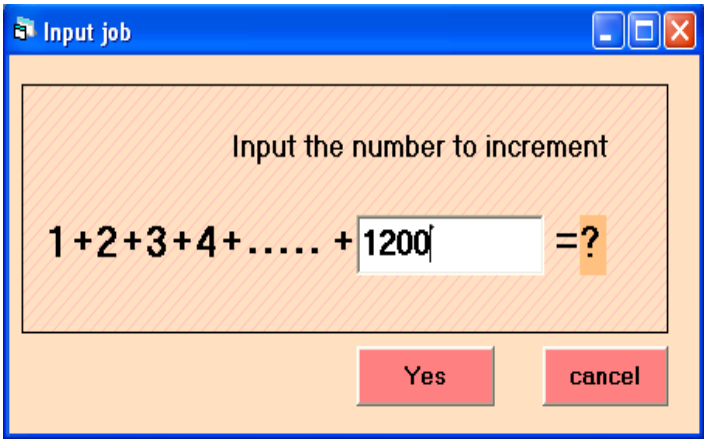


Fig. (8) Input of the job

Step 7:- run the job by entering the number we want the loop counts.

Step 8:- after 125 second, making active node 1 busy (by entering a CD in to the CD Drive which has the priority), the packet size become 15.360 and the packet travel to active node 2 and so on till the job is finish. An example is shown in **Table 2**. The active packet travels between the active nodes arbitrary by making the other nodes busy.

THE FINAL RESULT

It is clearly shown that each active node continue doing the Job as shown in **Table 1** until we make it busy (by entering a CD in to the CD Drive) and then other active node will take the Job and continue it and so on. The size of the packet increased each time the active node changed until the Job finished as shown in **Table 1**. The relationship between the time and the packet size are shown in **Fig. 9**.

Table 1: Time and size of packet lifecycle for all active nodes

Computer Name	Time lifecycle Packet in seconds	Size of Packet in KB
Computer 1	**125**	**15.360**
Computer 2	**134**	**15.872**
Computer 3	**90**	**16.384**
Computer 6	**153**	**16.896**
Computer 3	**112**	**17.408**
Computer 2	**234**	**17.920**
Computer 5	**120**	**18.432**
Computer 1	**32**	**18.944**

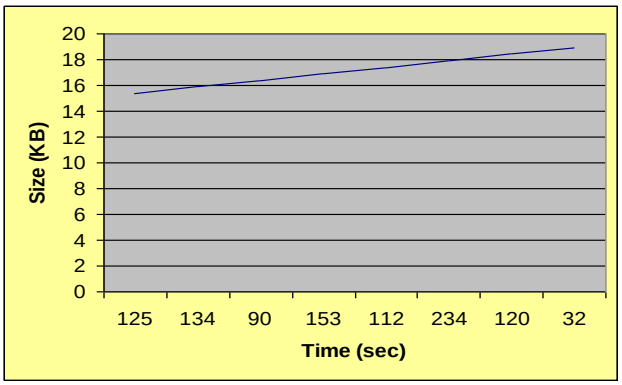


Fig. (9): The relationship between time and packet size

Table 2:
Example for the lifecycle Packet in Active Network for all Active Nodes is to travel.

8	7	6	5	4	3	2	1	
Ahmed	Ali	Wisam	Sara	Sama	Sara	Wisam	Ahmed	Username:
computer 1	computer 5	computer 2	computer 3	computer 6	computer 3	computer 2	computer 1	Computer Name:
1024 x 768	1024 x 768	1024 x 768	1024 x 768	1024 x 768	1024 x 768	1024 x 768	1024 x 768	Screen Resolution:
32 seconds.	120 seconds.	234 seconds.	112 seconds.	153 seconds.	90 seconds.	134 seconds.	125 seconds.	Windows Running time:
C:\both\C1	C:\both\C1	C:\both\C1	C:\both\C1	C:\both\C1	C:\both\C1	C:\both\C1	C:\both\C1	Program Location:
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Sound Enabled:
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Screensaver Enabled:
Windows XP	Windows XP	Windows XP	Windows XP	Windows XP	Windows XP	Windows XP	Windows XP	OS Platform:
5.01	5.01	5.01	5.01	5.01	5.01	5.01	5.01	OS Version:
187.178.128.21	187.178.128.25	187.178.128.22	187.178.128.23	187.178.128.26	187.178.128.23	187.178.128.22	187.178.128.21	Local IP:
Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Communicating with a device:
AC Adaptor	AC Adaptor	AC Adaptor	AC Adaptor	AC Adaptor	AC Adaptor	AC Adaptor	AC Adaptor	Current Power Supply:
No Battery	No Battery	No Battery	No Battery	No Battery	No Battery	No Battery	No Battery	Battery status

CONCLUSIONS

- From the results obtained from the test of the proposed system we can conclude:-
- Systems flexibility is very high, since the system can perform a variety of tasks and remain efficient.
- The security power of proposed system comes from different security tools (Authentication, Authorization and RSA algorithm), which reduce the possibility of hacking the information since the attacker has to defeat all those tools.
- The performance of proposed system is good because the throughput is displayed in the first active PC when packet started, and carries information of each node it visits.
- Cost in
    - Time (because more time spend on the cryptographic operation).
    - Packet overhead.
- The weakness of using password, which can be stolen, accidentally revealed or forgotten.

REFERENCES

- Bhattacharjee S., "Active Networks: Architectures, Composition and Applications", a PhD Thesis, Georgia Institute of Technology**,** 1999.
- Calvert K. L., "Architecture Framework for Active Networks", a PhD Thesis, Georgia Institute of Technology, 1999.
- Eva H., and Ludek K.,"Active networks and high speed content delivery", Proceedings of the The 7th International Conference of European University Information Systems on The Changing Universities - The Role of Technology, Vol. 13, PP. 448-456, 2001.
- Gert D. L., and Gert S., "Network Security Fundamentals", Cisco System, Inc. published by: Cisco press, 2005.
- **http:// www.ciscopress.com/bookstore/product.asp?isbn=1587051672**
- Jean-Patrick G., "Towards the design of an active network architecture supporting throughputs of gigabit networks", a PhD Thesis, University of Tennessee, December 2003.
- Laat C. de, Gross G., Gommans L., Vollbrecht J., and Spence D., "Generic AAA Architecture", IETF Network Working Group, Internet experimental RFC 2903, August 2000.
- **http://tools.ietf.org/html/rfc2903**
- Ravi S. and Pierangela S., "Authentication, Access Control, and Audit", ACM Computing Surveys, Vol. 28, No. 1, March 1996.
- Psounis K., "Active Networks: Applications, Security, Safety and Architectures", IEEE Communications Surveys and Tutorials, Vol. 2, No. 1, PP. 2-16, First Quarter 1999.

- Tennenhouse D. L., Sincoskie W. D., and Wetherall D. J., "A Survey of Active Network Research", IEEE Communication Magazine, Vol. 35, No. 1, PP. 80-86, January 1997.
- Tennenhouse D. L.**,** and Wetherall D. J., "Towards an Active Network Architecture", DARPA Active Networks Conference and Exposition, San Francisco, CA, USA. IEEE Computer Society 2002, PP. 29-31 , May 2002.
- Wetherall D. J., "Active network vision and reality: lessons from a capsule-based system", 17th ACM Symposium on Operating Systems Principles (SOSP '99) Published as Operating Systems Review Vol. 34, No. 5, PP. 64–79, Dec. 1999 .