# Implementation of PadSteg: A new Steganography method

Dhanashri D. Dhobale
*Assi. Prof P. V. P. I. T. Budhgaon*
*Sangli, India*

Dr. Vijay R. Ghorpade
*Principal, D. Y. Patil College of Engg.*
*Kolhapur, India*

**Abstract - The work relates the area of Stegenography, network protocols and security for data hiding in communication networks. Hiding information in network traffic may lead to leakage of confidential information. Steganography is defined as the art and science of hiding information, which is a process that involves hiding a message in an appropriate carrier for example an image file. The carrier can then be sent to a receiver without anyone else knowing that it contains a hidden message.**

**Implementation of new Stegenography, the PadSteg (Padding Stegenography) system is implemented. It is the first information hiding solution which represents inter-protocol steganography i.e. usage of relation between two or more protocols from the TCP/IP stack to enable secret communication. PadSteg utilizes ARP and TCP protocols together with an Ether leak vulnerability (improper Ethernet frame padding) to facilitate secret communication for hidden groups in LANs (Local Area Networks). Proposed work is to confirm that PadSteg is feasible in today's network and it provides more security within secret group.**

**Keywords: Stegenography, ARP, improper padding, Ether leak vulnerability.**

## I. PROPOSED EXPERIMENTAL WORK

The implementation of PadSteg is proposed to design steganographic system in 2 stages:

1. Advertizing of New node and adding it in secret group.
2. Hidden data Exchange with more security.

## II. LITERATURE SERVEY.

Network steganography is currently seen as a rising threat to network security. Contrary to typical steganographic methods which utilize digital media (pictures, audio and video files) as a cover for hidden data (steganogram), network steganography utilizes communication protocols' control elements and their basic intrinsic functionality. As a result, such methods may be harder to detect and eliminate. In order to minimize the potential threat to public security, identification of such methods is important as it is the development of effective detection (steganalysis) methods. This requires both an in-depth understanding of the functionality of network protocols and the ways in which it can be used for steganography.

Many methods have been proposed and analyzed for network Stegenography. Steganography by hiding data in TCP/ IP headers is the system in which TCP/IP headers are utilized for Steganography purpose. But it can be easy to detect the system because of the single protocol utilization. Also such single protocol systems dosent provide more security.

So, the new technique Padding Steganography (PadSteg) is the new technique which is an inter protocol Steganography. Here multiple protocols ARP, TCP and ICMP are utilized for secret communication. Also this system cannot be easily detected and it provides more security than previous systems.

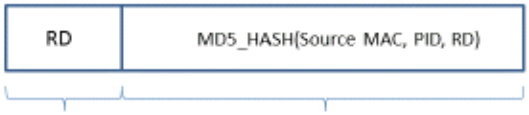
## III. EXPERIMENTAL MODULES AND SETUP.

A detailed study of literature has been carried out to work further. For the implementation of all modules mentioned in synopsis some basic steps are required. Following are the basic steps required for project.

PadSteg system is based on the Ethernet frames for Communication. In order to establish communication, you must understand the following –

Steps: 1. initialization of the hidden node/nodes, who wants to pursue a communications, distributes modified ARP-Request. In the message frame padding information can be found that allow different nodes of the network about the existence of the mailer.

Padding:
a) Random number RD.
b) The result of a computed hash function based on the value of the RD, the MAC address of the sender and the protocol identifier is PID media




Step 2 Exchange of data – to determine which protocol will be followed a communication, data exchange can be started. For example, if it was TCP, hidden information can be placed in the ACK message sent during the transfer of files between nodes.

The work is divided in 5 modules. First module consists of finding interfaces and advertising its availability by sending an ARP request to all available nodes.

## IV. GENERATED RESULTS AND OUTPUTS.

*User Interface I:*

After executing the project screen as shown in Fig. 1 is displayed. This screen shows all the network interfaces to the communicator. Here in fig we see only one interface which is available and it has given ID 0. If more interfaces then all will be displayed here.

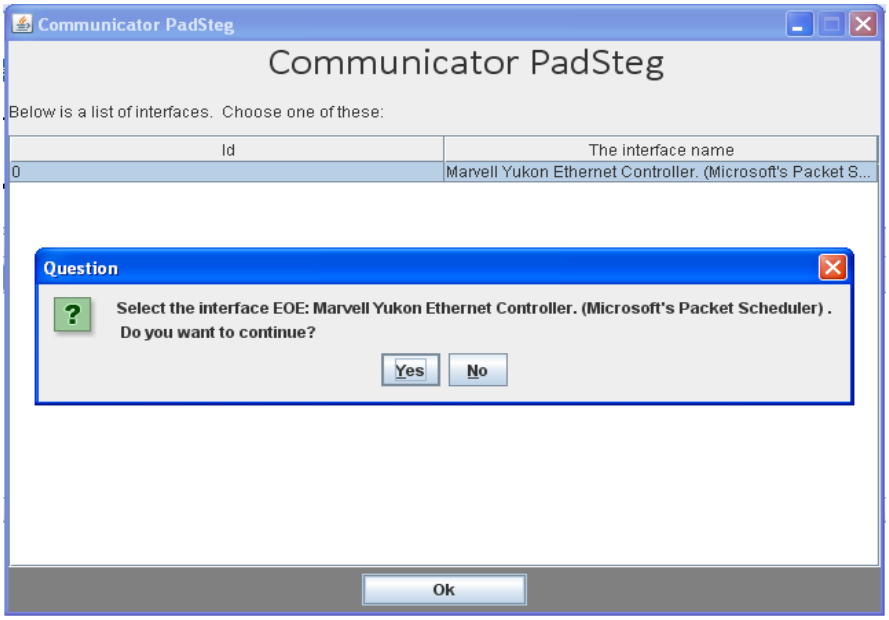



Fig-1 – Finding interfaces.

After selecting the interface in above screen and clicking OK the ARP request is sent to all the nodes along with the MAC address with padding bits of ARP. This is to tell about its availability to other communicators for further communication.

*User Interface II:*

The screen in fig 2 shows sending of ARP along with information. We have source MAC address , source IP address and Interface name. The ARP is sent to all the nods which are padsteg enable nodes where ARP request consists of the HASH Key which is generated by applying MD5 HASH function on source MAC address, RD (Random No.) and PID. This is done by:

**Hk = MD5 (RD, Source MAC, PID)**

Where RD is a random number generated, PID with one of the following values:

| Protocol | PID | Purpose |
|---|---|---|
| TCP | 1 | communication using TCP |
| ICMP | 2 | Communication using ICMP |
| ARP | 3 | Message Availability |

When the request is sent the communicator is ready to talk with requested communicator.The screen will display having all connected and reachable nodes. The PadSteg enabled nodes are indicated by giving their status as “Available” and those are not are indicated by “Not available”. In Fig 2. MULT1 and MULT2 nodes are with status “Available” indicating PadSteg enabled nodes.

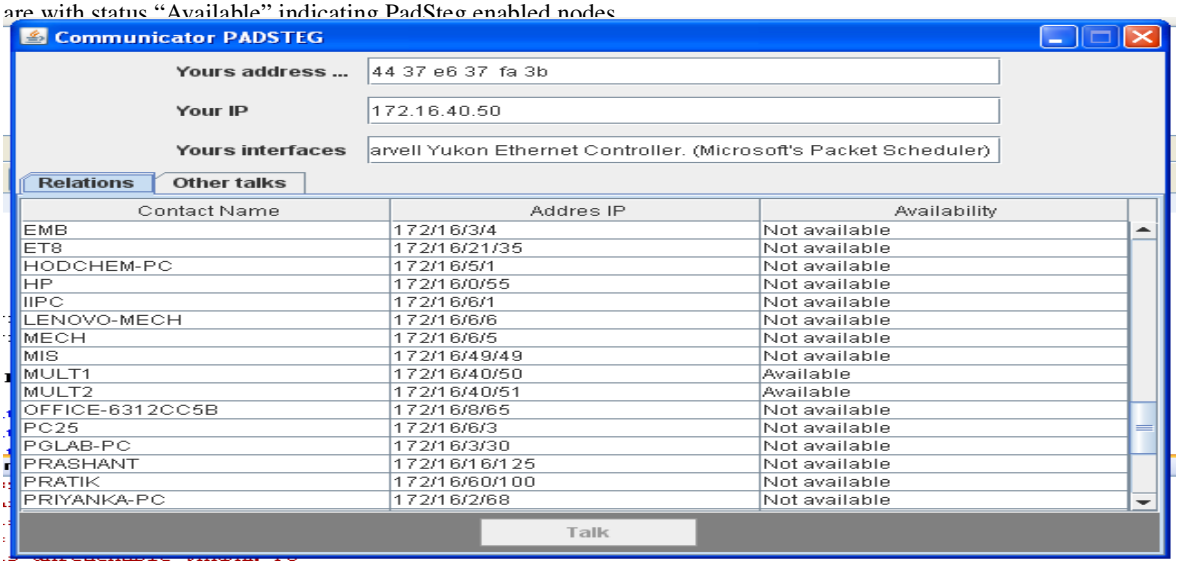



Fig 2- Sending ARP along with information like MAC address through padding .

*User Interface III:*

After getting PadSteg enabled nodes select node for communication.The project screen as shown in Fig. 3 is displayed, which gives the list of all reachable and PadSteg enabled nodes. MULT1 and MULT2 are PadSteg enabled nodes. In fig 3. MULT2 is selected for communication.

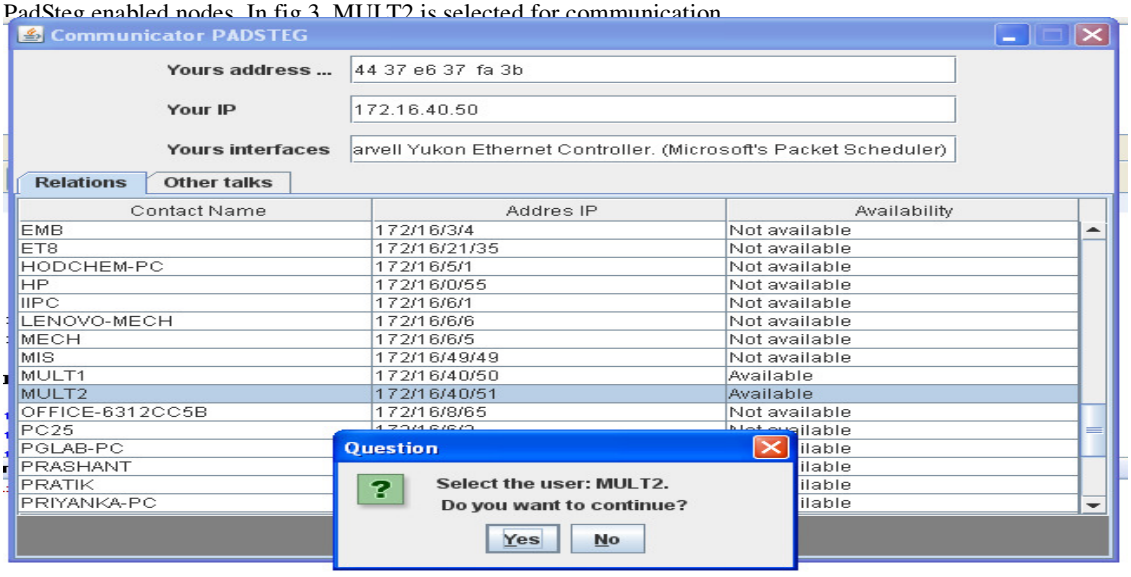



Fig. 3- Screen showing selection of PadSteg enabled node

*User Interface IV:*

Sending an ARP request indicating PadSteg Communication request.

As shown in Fig. 4 the ARP request is sent to the other PadSteg enabled node as an request for PadSteg Communication.

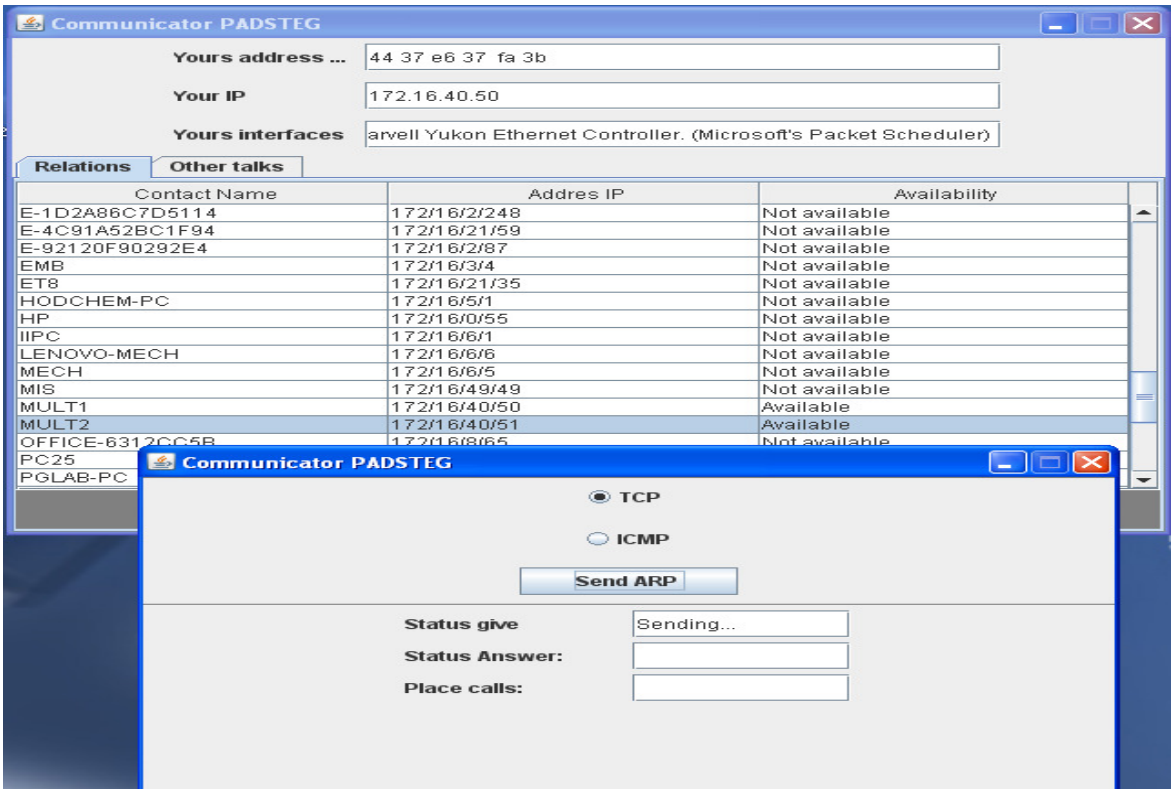



Fig-4 – Sending ARP request for PadSteg communication Request..

*User Interface V* :

After getting ARP Request sending analogical reply for communication from other node. Here after receiving the Request ARP packet the PadSteg communication reply is sent through ARP packet. This is shown in Fig. 5

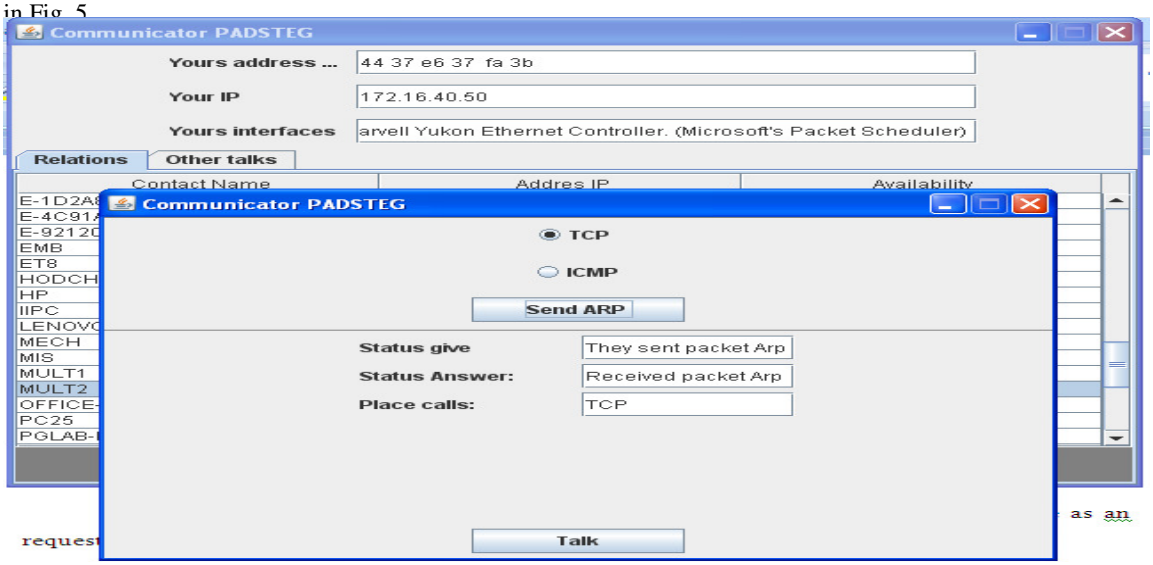



Fig. 5 Sending acknowledgment for PadSteg Request.

*User Interface VI:*

After getting analogical reply, request to perform actual talk with PadSteg.

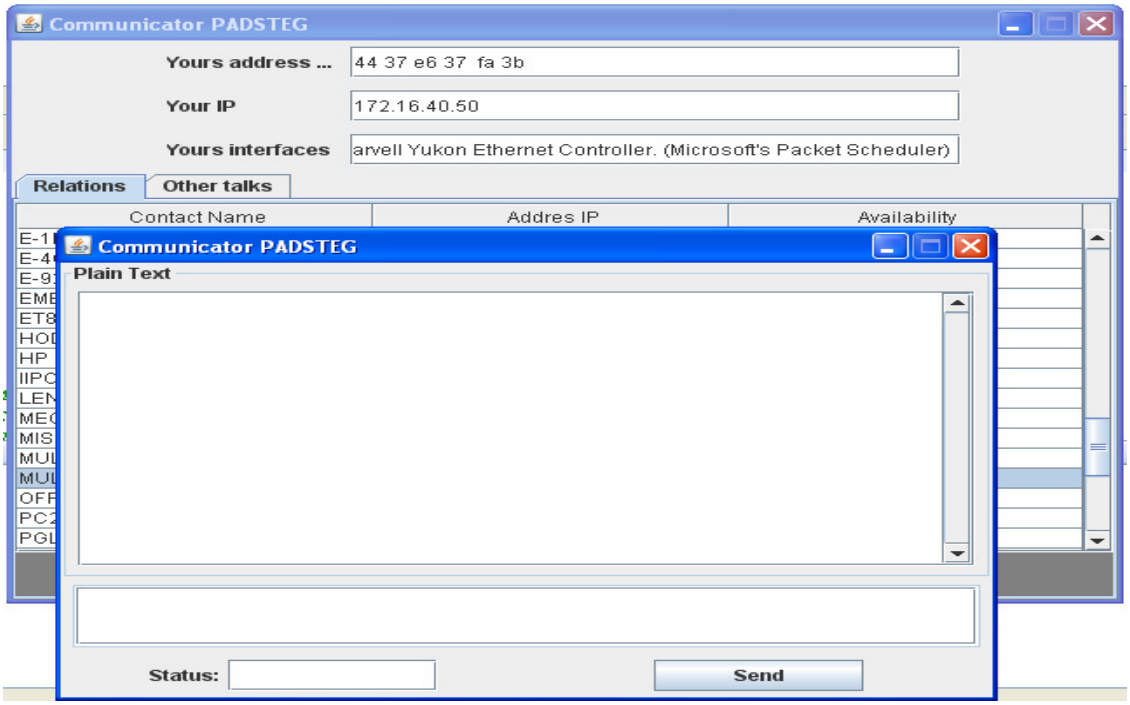



Fig. 6. The screen providing the PadSteg talk.

## V. PADSTEG COMMUNICATION :

After group formation and connection establishment following steps are followed to do the PadSteg communication.

*Sending plain text from sender.*

Here in this step the actual PadSteg communication starts. The default protocol for the communication is TCP. When the link for communication is generated the sender sends the encoded plain text to receiver through the padding bits of TCP. The receiver then receives the sent message and again can send message to the node on another side. Hence the communication starts like the chatting.

*Receiving plain text sent by sender.*

When receiver receives the mesage it extracts the message and decodes it. Also the message can be sent through same process by encoding and Decoding.

*Changing practical protocol from TCP to ICMP.*

For more security the user or sender can change his ttransmission protocol from TCP to ICMP. So that it cannot be detected by third person. So for this process it is requires to change the protocol type from TCP option to ICMP option. After the pinging is required for ICMP protocol. Now its ready for PadSteg communication through ICMP.

*Performing communication through ICMP protocol.*

In this step the user can send his secret message through PadSteg using ICMP protocol. Hnce the method is Very hard to detect.

## VI. CONCLUSION

Hence the system impleted said PadSteg is a secure process . We can use this system for the secret communication in a LAN. As multiple protocols are used for communication the system is very hard to detect. Also during communication process the practical protocol can be changed , so again it provides the more security which is very hard to detect.

## REFERENCES

[1] Petitcolas F., Anderson R., Kuhn M., Information Hiding – A Survey: IEEE Special Issue on Protection of Multimedia Content, July 1999.

[2] Mazurczyk W., Smolarczyk M., Szczypiorski K.: Retransmission steganography and its detection, Soft Computing, ISSN: 1432-7643 (print version), ISSN: 1433-7479 (electronic version), Journal no. 500 Springer, November 2009.

[3] B. Jankowski, W. Mazurczyk, K. Szczypiorski, Information Hiding Using Improper Frame Padding, Submitted to 14th International

Telecommunications Network Strategy and Planning Symposium (Networks 2010), 27-30.09.2010, Warsaw, Poland.

[4] B. Jankowski, W. Mazurczyk, ~~K. Szczypiorski~~ - *PadSteg: Introducing Inter-Protocol Steganography* - In: Telecommunication Systems:

[5] ~~**www.stegano.net** http://jnetpcap.com/tutorial~~.

[6] Java Network programming – 3rd edition.

[7] Steganography by hiding data in TCP/IP headers, IEEE International Conference ICACTE, China, 2009.

[8] Published paper on " An overview of advanced network protocol steganography" in an I'national journal IJARCCE, Volume 2, Issue 9, September 2013, **Impact Factor- 1.770** ISSN (Online): 2278 – 1021 ISSN (Print): 2319 – 5940.