LOVELY PROFESSIONAL UNIVERSITY

Transforming Education Transforming India

REPORT OF RESEARCH PAPER

ON

A Review study on Covert Channel Attacks

Submitted to

LOVELY PROFESSIONAL UNIVERSITY

In partial fulfillment of the requirements for the award of degree of

Master in Computer Applications

Submitted By:

Aman Tyagi

Reg.No:11401252

Supervised By:

Mr.Parvesh Mor

LOVELY FACULTY OF TECHNOLOGY AND SCIENCES

LOVELY PROFESSIONAL UNIVERSITY

PUNJAB

Index

Acknowledgement

I place my sincere thanks to my teacher Mr.Parvesh Mor for his supervision and advices to complete my work successfully. I also thank our HOD Mr.Balraj for providing me all the facilities to finish the term paper on time. My *RESEARCH PAPER* report on “Covert channel Attacks” acknowledgement I would like to take this opportunity to express my gratitude towards all the people who have in various ways, helped in the successful completion of my term paper.

Introduction

Today, system security has become top priorities of all organization because if their system will become victim of any type of attack then there is a risk to organization's data, network, etc. Among all types of attacks the covert channel attack becomes the biggest problem of system security because it is a hidden threat. It is a type of mechanism of sending and receiving a message without alerting firewall and IDS (Intrusion Detection System).

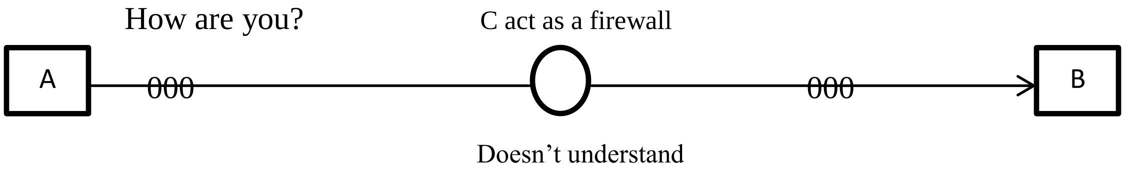

Fig1.Simple example of covert channel

In Fig1 A and B are two person live in different hostel and they want to communicate but, there is a warden C which act as a firewall or IDS if they send a simple message then warden read a message and don't allow to forward it. So, they have to communicate each other in code like: 1 for even number and 0 for odd number of words suppose the message is "Hey, what is the plan of tomorrow movie?" so the code is "01101110" by this C can't understand this code and they both able to interact. So, in this paper I will read the review of different papers and on the basis of them I will give the own methodology which describe how we can prevent covert channel attack efficiently.

Literature Review

R.Trimble *et. al.* has discussed about Covert channels that what is the purpose of implementing of this hidden threat? This is a problem for a system administrator and it is not easy to detect.

This Paper defines why anyone can implement covert channel very easily in any network because security professionals are busy in detecting the viruses, Trojan horses and other various exploits for these reasons covert channel were hiding or understanding as not important. Its low priority covert channel exploited by a process that transfer information in a manner that the system security policy.

Purpose of these attack stolen the data and information .A channel is only consider malicious if it is banned by the security policy.

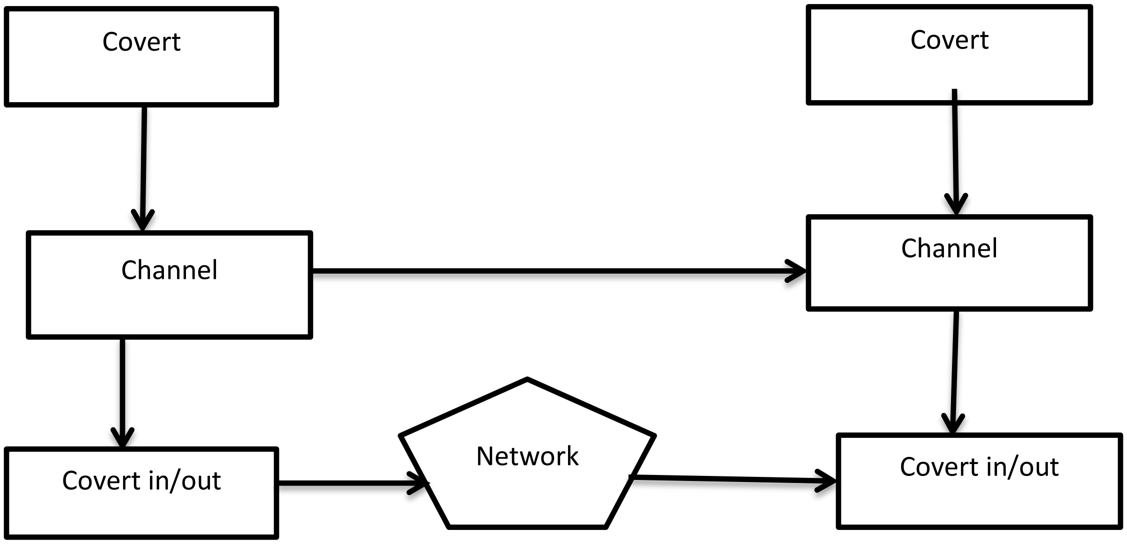

Fig.2 Process of covert channel

Hamed O.Kharvi *et.al.* had explained about covert channel threat to the security of critical infrastructure and key resource. That defense and countermeasure against this threat. Paper defines covert channel attack is depends on network. Other class of covert channel hardware and system are based on these attack, the attackers can use such a techniques to leak sensitive information that are probably correct.

A sender and receiver using the network may both read or write in used IP bit field.

Table 1. Covert Channel Attacks

Attacks	**Description**
Transition based attack	A hardware device can store a value both processes can view
Hardware timing value based attack	Sender has executed or invoke right over the receiver.
Operating system Storage transition based attack	Sender cannot change the state to obituary values this uses the file system.
Operating system timing value based attack	Uses the system timer as shared resources.
Hybrid covert channel design and implementation	Receiver Check at this counter for checking the packet has been sent or not.

E.Pennington *et.al.* Discussed methods of communications that is used to transfer information between senders to receiver. That breaking the system security policy of any system .This is the method of covert channel like: Brute force password attack to port scanning.

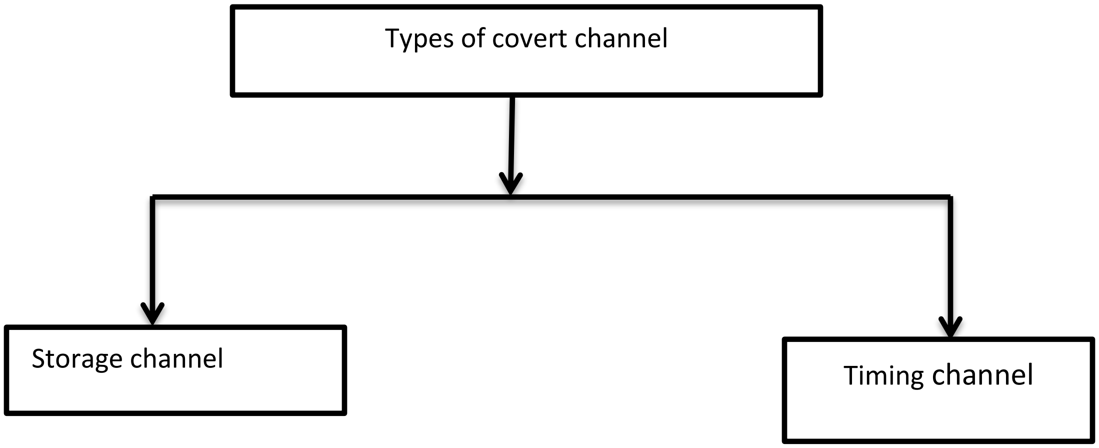

Fig.3 Types of covert channel

Storage channels are method of communication that is a storage location by one process of the direct and indirect reading access. Purpose of storage channels can be used between processes within a single computer access a network.

Wade c.gasior *et.al.* discussed mobile device such as: smartphones and tablets have become a ubiquitous computing and storing or access to a large amount of sensitive information.

This paper shows prime device of targets. Attacker can attack with some malicious intent. The implements of network covert channel on the android mobile platform, and show that data can be leaked form these devices in a manner that devices is not undetectable by the user, phones security features or network security between the mobile device and the other network.

A network channel attack is use of a shared secured ,a network communication channels to transfer information in which it was not initially designed for secure protraction techniques such as firewalls ,encryption detection system of instruction.

Table 2 challenges & phases of covert channel Attack

Phases	**Challenges**
First	System requires application to request permission from the user.
Second	Android platform does not allow an application to have access to raw packets.
Third	This is difficult of implementing timing-based convert channel other cellular network.

Swarup Chandra *et.al.* Discussed the smartphone security and numbers of users and range of application and provide the mechanism for data protection by restriction of the communication between applications with in devices. Malicious applications still overcome such restriction via such vulnerability in systems or using covert channels for the purpose data transferring.

Android operating system inherits the Linux security infrastructure there application are installed and executed with in its individual. An attacker interested in obtaining user’s private illegal access. A covert channel can be used by malicious application for such as an attack.

Table 3. Types of covert channel, Technology and their results

	Paper 1	Paper 2	Paper 3	Paper 4	Paper 5
Technology introduced	Covert channel and They risk perform to the integrity of the system.	Covert channel designed attack in real system presenting threat models bit rate.	Covert channel is a storage location, one process the direct or indirect reading of it by another.	Android platform in a way that is difficult to detection challenges.it is implemented own TCP and UDP protocols.	In covert channel analyzed various shared recourses be potentially exploited to transfer data maliciously.
Types of covert channel	Timing Channel. Storage Channel. Baby hacker method. (Encryption algorithm)	Transition-Based Attack. Hardware Timing value-Based Attack. Operating System Storage Based Attack.	Timing Channel. Storage Channel.	Timing-Based Covert Channel. Covert Storage Channel.	Phone Call Log Phone Call Frequency Screen Audio (Volume)
Result	From encryption to Steganography is a threat to any system. It impact on computer or same network and different network.	Covert channel capacity hardware device store a value that can view.	It implemented within a single computer or multiples computer across a network	Currently proposed covert channel detection and mechanism are not suitable for mobile platforms.	

Methodology

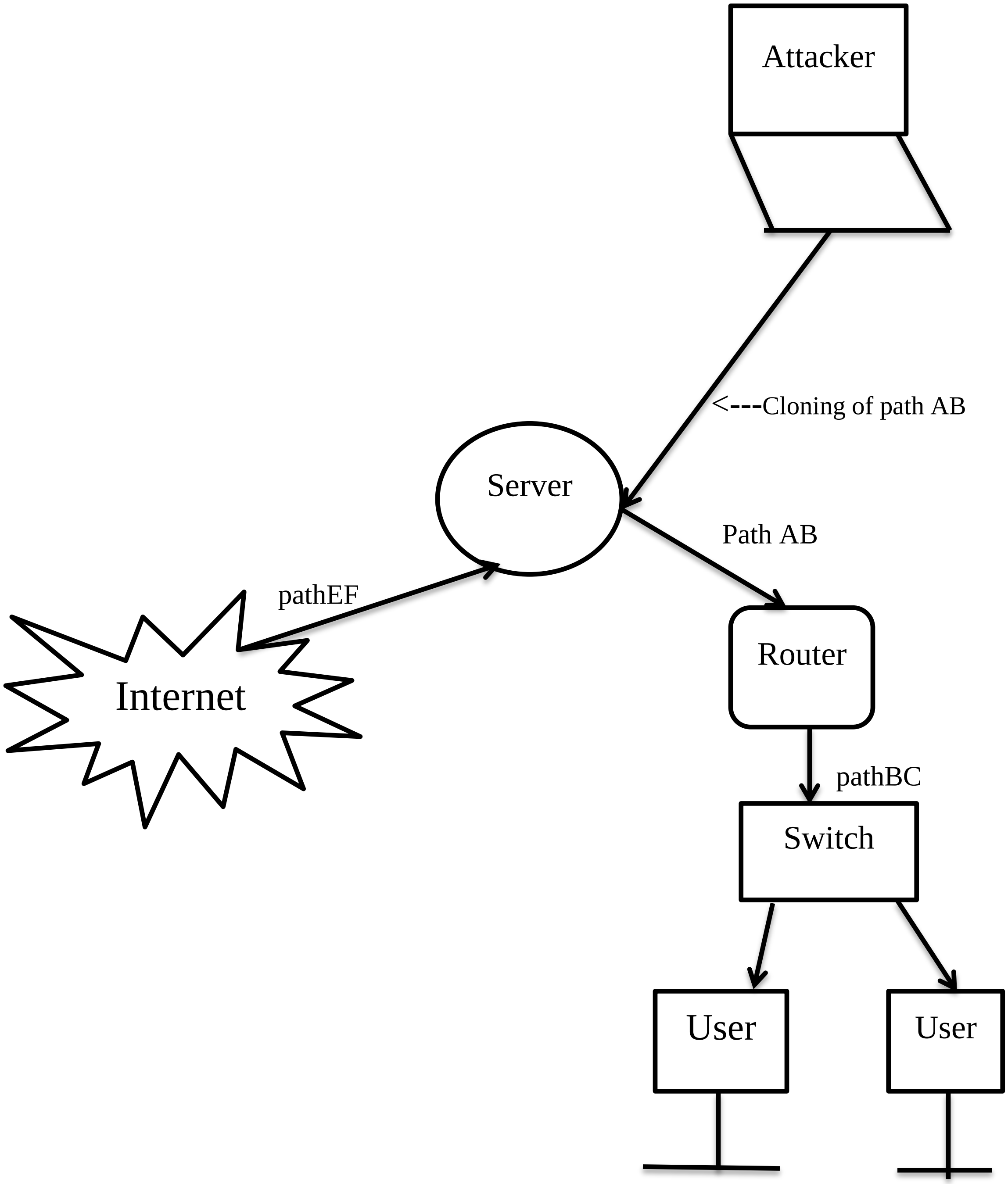

Fig.4 Path Cloning Covert Attack

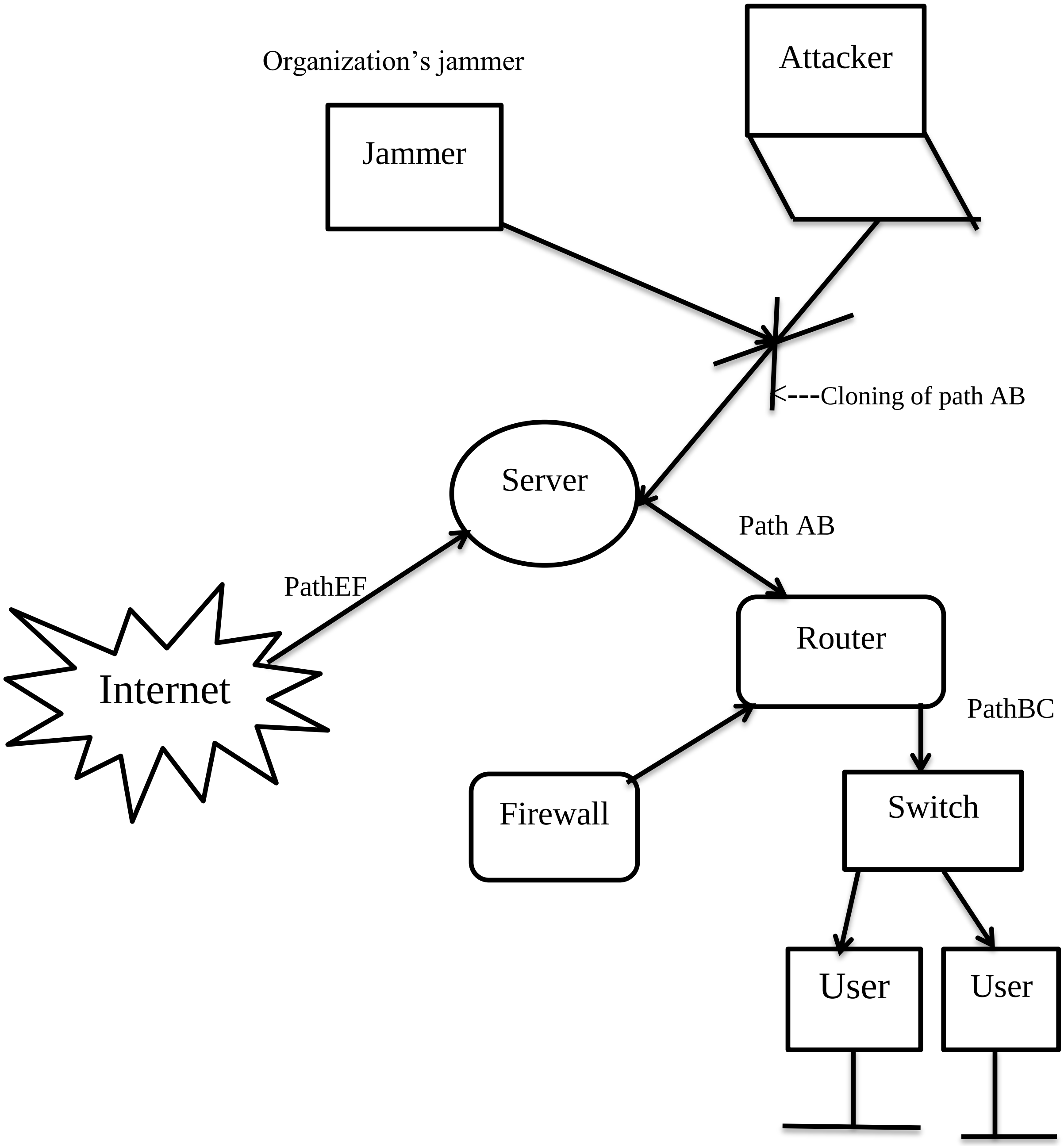

Fig.5 Prevention of Path Cloning Covert Attack using firewall & Jammer

In Fig 4.there are various points in which I will describe that how the users take information from internet & in Fig 5. How users' connection line become the victim of covert channel attack:

- The users send a SYN request to the server through the router then server & server fetch the information from the internet.
- The information go through the path EF to server, then server pass it to the router through path AB which is the less secure area.
- By this the user can get the legitimate information what he/she requires.

But is very easy to attack on a communication path AB between server & router by making the clone of a path AB. Suppose:

- When the information travelling between server and router the attacker which try to get the information will make the clone of path AB.
- After cloning, he/she implements its clone path AB between server and router by which server does not require any individual identification and transfer all information through that clone path AB.
- It is very risky for organization because, the attacker can control its clone and can modify the information by itself. By which user can get many difficulties for information.

It is very difficult to detect covert channel attack because it works same as our genuine communication path does. So, in Fig 5. for this problem I give a method to prevent it by including some points.

- As we know, during transferring the information between server and router the attacker can attack by cloning. So, we can implement a smart jammer which can block the cloning of the path AB.
- The working of smart jammer is like that at random time the jammer asks every communication path to give their identity by their owner as given in fig 5.
- Every owner has to give their identification when the jammer demands. If anyone unable to give the identification of their path then the jammer will block that path.

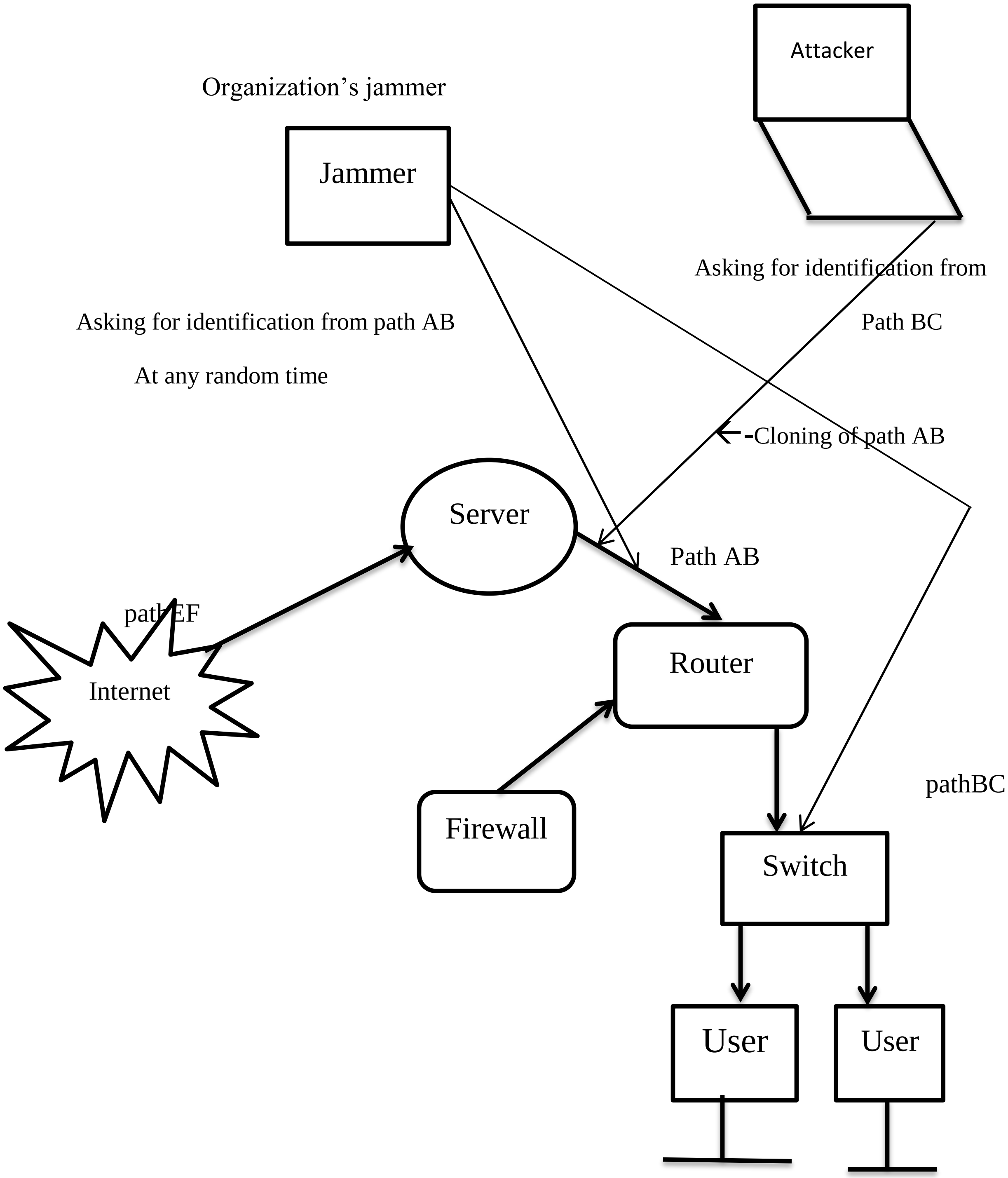

Fig6.Working of jammer in origination for detection of path cloning.

- In case of cloning path the jammer will ask for identification & the attacker unable to give identification & jammer will block that cloned path as shown in Fig6.

Conclusion

The covert channel attack is hidden threat in which the victim doesn’t know that his channel has been attacked by an attacker. The properties of covert channel are existence, covertness, capacity and by these properties it is difficult to detect covert channel. For this I have given a review that how can we detect covert channel attack and how can we resist this attack. In further, I will implement my methodology and optimize the output of prevention against covert channel attack. This technique can be implemented in the communication channel of an organization system to prevent cloning. But in this technique it is not mandatory that attacker will attack over the communication channel of server because it is depend on attacker where he wants to attack like: maybe he can attack on path BC maybe he can on path YZ so, this can be a drawback of this method.

.

References:

[1] R. Trimble, W. Oblitey, S. Ezekiel, J. Wolfe: “Covert Channels: The Hidden Threat”, Covert Channels Research Group, IUP Computer Science Department,319 Stright Hall IUP, Indiana PA 15705

[2] Hamed Okhravi, Stanley Bak, Samuel T. King: “Design, Implementation and Evaluation of Covert Channel Attacks” Department of Electrical and Computer Engineering University of Illinois at Urbana-Champaign Urbana, Illinois 61801.

[3] E. Pennington, W. Oblitey, S. Ezekiel, J. Wolfe: “An Overview of Covert Channels” Covert Channels Research Group, Computer Science Department IUP, Indiana, PA 15705.

[4] Wade Gasior and Li Yang: “Exploring Covert Channel in Android Platform” University of Tennessee at Chattanooga, TN USA.

[5] Swarup Chandra, Zhiqiang Lin, Ashish Kundu, and Latifur Khan: “Towards a Systematic Study of the Covert Channel Attacks in Smartphones” The University of Texas at Dallas, Richardson, TX, USA, IBM T J Watson Research Center, NY, USA.

[6] JingzhengWu, YanjunWu: “C2Detector: a covert channel detection framework in cloud computing ”: National Engineering Research Center for Fundamental Software, Institute of Software, Beijing, China, North Dakota State University, Fargo, ND 58108-6050, USA.
.

[7] Sebastian Zander, Grenville Armitage: “Covert Channels and Countermeasures in Compute Network Protocols” Philip Branch Swinburne University of Technology.

[8] Kirti Chawla, Gabriel Robins: “Addressing Covert Channel Attacks in RFID Enabled Supply Chains” *University of Virginia, USA.*

[9] Daryl Johnson, Bo Yuan, Peter Lutz, Erik Brown: “Covert channels in the HTTP network protocol: Channel characterization and detecting man-in the-middle attacks ” .