# Bi-Directional Mapping With Threat Ontology

Seema[1], Bhawna Mallick[2]

[1]Dept. of Computer Science, [2]Head of the Department(Dept. of CS & IT)

[1,2]Galgotia College of Engineering and Technology, Greater Noida

***Abstract - Our generation is using IPv4 which is 32 bit protocol which seems having shortage of addresses .To resolve the various problems of ipv4,new protocol is in research which is named as IPv6.IPv6 have various features which make it superior than IPv4 like multicasting, expanded address spaces, automatic network configuration, security feature (IPsec), guaranteed communication quality. To make data transition from IPv4 to IPv6 or from IPv6 to IPv4 there are various methods dual stacking ,tunnelling ,translation mechanism, bi-directional mapping system .In this paper .We propose a bi-directional mapping system with having security in mind, for security we use ontology based anti-threat decision support system for IPv4/IPv6.As the security is major concerned now-a-days this decision support system will make IPv6 protocol more convenient to use.***

***Keywords: Ontology, Anti-Threat, IPv6, Bi-Directional Mapping System.***

## I. INTRODUCTION

The tremendous growth of internet is becoming a problem like lacking of ipv4 addresses, lack of security. To overcome these problems ipv6 came in existence which has inbuilt IPsec function for security. In ipv6 security challenge is still at risk for the host, survey conducted by the community of network security has revealed that no 1 risk is to have lack of knowledge about the new protocol (ipv6)[1].

For transition to be made in ipv4 network step by step methods of transition were proposed for smooth transition [2].by managing the co-existence of ipv4 and ipv6 .there is a risk of security management. Transition of ipv4/ipv6 to be done securely is major concern no a days. The transition method which we are using in this paper is bi-directional mapping transition system.it is very simple, easy to be implemented, efficient, it reduces the packet size than tunnelling mechanism and reduces cost of ipv6 than dual stack mechanism[3].

Bidirectional mapping system is operated when host in the network of ipv4 initiates connection to the host of network of ipv6.It depends on the following components:

1. v6-v4 domain name system: it identifies the network addresses dynamically or statically for ipv4/ipv6 session.

2. v6-v4 enabled gateway: it performs the address mapping between the two networks, it also performs the header conversion between ipv6 and ipv4 packet header.

*A. BDMS main criterias are*

- *It reduces the traffic overhead by reducing the packet size as compared to tunnelling mechanism [3].*
- *By avoiding upgrading of all edges, it reduces the cost of ipv6 as compared to dual stack mechanism [3].*

To solve the security problem in bi-directional mapping this paper study proposes the anti-threat ontology of ipv6/ipv4 to make networks secure.

## II. RELATED WORK

To understand the security feature of ipv6 we have to understand how to solve security issues in network ipv4.As we all know ipv4 does not have any security; there are some characteristics which allow different types of threat to take off:

- Denial of service attack: this attack sends illegal request to make service unavailable.
- Man-in-the middle attack: in this attack due to lack of authentication data is intercepted by the attacker.
- Fragmentation attack: IP fragmentation mechanism is used in this attack.
- Icmp redirect and ARP positioning attack: in this attack spoofed address protocol is send to the local network area and sends it to the attacker rather than to host.
- Malware distribution attack: host is infected in this attack by distribution of malware.
- Reconnaissance attack: To find unpatched services, this network scan whole network.

Ipv6 is not just an improvement to ipv4 but it is actually a new protocol with advanced features like larger address space, IPsec, neighbour discovery protocol, multicast which replaced broadcasting of ipv4 and extended header with having maximum transmission unit (MTU) [4].

Ipv6 improves ipv4 but caicedo and joshi[5] revealed various attacks like reconnaissance, host-initialization, attacks through routing header, attacks based on multicast.

Transition technology like translation system, dual stack and tunnelling, bi-directional mapping system have new security issues. Thus this issue should be outlined to make new policies of issues related to security. How to resolve issues is becoming a challenge.

## III. TRANSITION MECHANISM

Ipv6 is advance protocol than ipv4 but to deploy ipv6 there is a need of ipv4 co-existence for a period of time to make ipv4 network users to allow using their old applications [6].Transition mechanism which are famous: tunnelling, dual stack, translation, bi-directional mapping system.

### *A. BI-DIRECTIONAL MAPPPING SYSTEM*

BDMS depends on identification of two public addresses (ipv6 and ipv4) for every communicating session, understanding of the received datagram, identifying and capturing the header, datagram transformation to the destination environment and then transmission of the datagram into address of the destination [3].

To make the policies for security issues ontology approach is selected to manage threats and knowledge of anti-threat. Our efforts are needed to remove these threats; by human skill and knowledge we will reach to the solution. Threat issue is very critical.

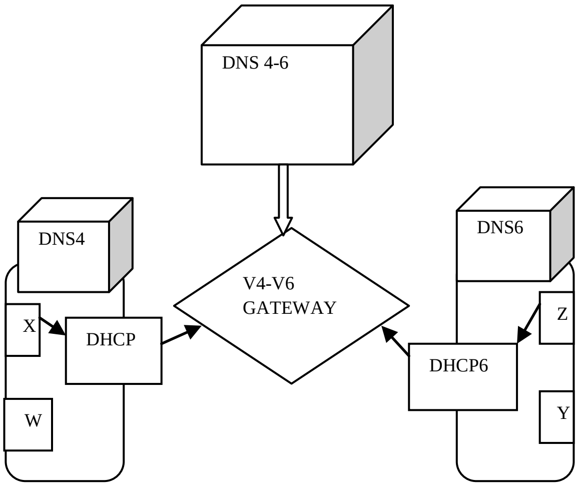

Fig 1. Bi-directional mapping system

### *B. DUAL STACK BACKBONE*

This is the mechanism by which there is a possibility of two stacks to be run in parallel.ipv6 and ipv4 protocol stack have to be maintained on all routers. There is not any translation between ipv4 and ipv6 because ipv6 application can communicate with host of ipv4 and ipv4 application can communicate with host of ipv6.Disadvantage of this mechanism is that there is need to upgrade all the edges to run two protocols[7].

### *C. TUNNELLING MECHANISM*

This mechanism is used when the hosts which want to communicate are located in ipv6 only zone and want to pass their packets through ipv4 only zone then to pass the packet ipv6 packet is firstly encapsulated into ipv4 packet so that it can be passed through ipv4 zone[3].

This mechanism allows ending system and routers of ipv6 to communicate through ipv4 infrastructure.

### *D. TRANSLATION MECHANISM*

This mechanism is very important and it is used when host and destination use different protocol then translator is used to make host packet understandable by converting packet according to destination example: host is using ipv4 packet whereas destination is using ipv6 packet and host want to send packet to destination then packet will be converted into ipv6 so that it can be understood by destination [3].

## IV. THE ONTOLOGY OF ANTI-THREAT KNOWLEDGE

To make successful policies for security requires attention to factors like cost, security risk, devices, sensitivity to threats.

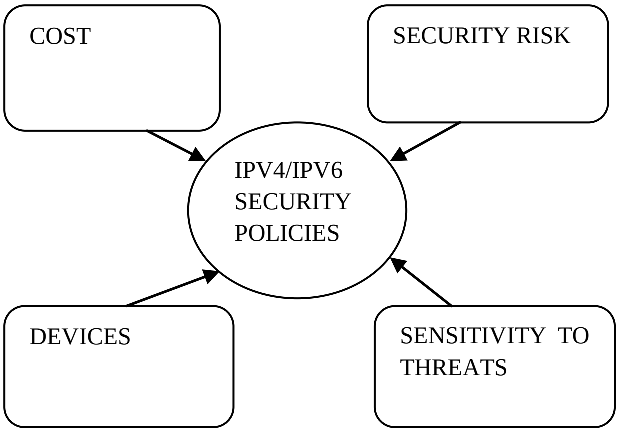

Fig 2. Factors of anti-threat policy

### *A. ANTI-THREAT ONTOLOGY*

Against the network threat, various technologies were proposed to detect and prevent Network vulnerabilities. Cost is needed to proficient security technology is an important factor to evaluate the threat risks. Ontology has three layers. The first and second layer contains various attack and threat techniques. The third layer is the security tools like deep packet inspection (DPI), intrusion detection system (IDS), firewall, net flow analyser, intrusion prevention system etc. [8].

When we talk practically, transition of ipv4 to ipv6 can be designed by four phases.

1. Phase network ipv4 with the experimental network of ipv6.

2. Phase network coexist Ipv6 Island and Ipv4 Ocean.

3. Phase network coexist Ipv6 Ocean and Ipv4 Island.

4. Phase network use only ipv6.

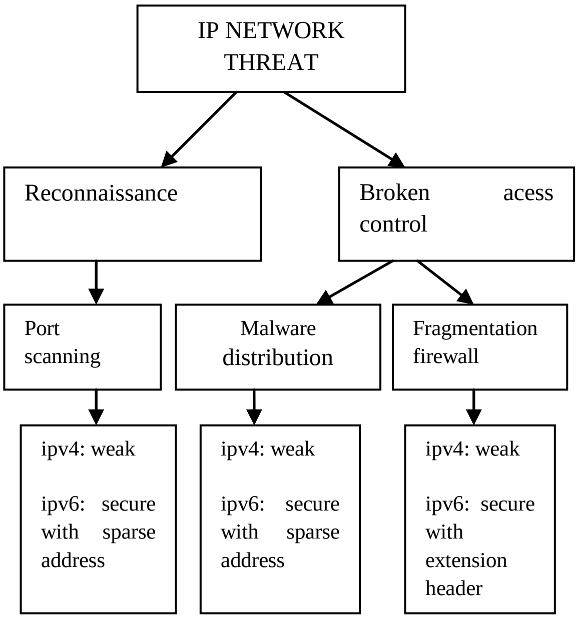

Fig 3. Ontology decision support

During these phases, configuration of network changes and different vulnerabilities are exposed. Thus this ontology based anti-threat decision system motive is to provide security to the different phases. The configuration attribute describe network as: ipv6 only, ipv4 only, translation, tunnel, dual stack. Attribute of network are WAN or LAN. Attribute of the service are DNS server, Web server-mail server. Possible threat information to the device provided by the first three attributes. Critical degree of various types attacks specified by the sensitivity of attribute of threats.

Each device has three states. To adopt new policies of security the state of initial network is transformed into state of trial network. If the anti-threat evaluation is passed by the trial network then the status will be changed to state of secure network. If the anti-threat evaluation is failed by the trial network then status is changed to the initial network. After that new policies of security will be conducted.

## V. CONCLUSION

In this paper ontology based approach is proposed to manage security knowledge of ipv4/ipv6.complications come when there is co-existence of ipv4/ipv6.to resolve these complications threat ontology is discussed to detect and resolve various attacks.in this paper we discussed how to use bi-directional mapping with security in mind. As BDMS is good mechanism for transition between ipv4 and ipv6 as it reduces packet size compared with the tunnelling mechanism, it also reduces cost by avoiding the up gradation of edge nodes.

In this paper it is proposed that bi-directional mapping is very good transition mechanism so we need better security policies to be made for this mapping system. For security ontology based approach is good by which this mapping can become very secure and can manage various threats.

## REFERENCES

[1] B.”Biggest risk in ipv6 security today” Network World http://www.networkworld.com/news/tech/2013/110413-ipv6, November o4, 2013.

[2] D. G .Chandra, M. Kathing ,D. P. Kumar ,” A Comparative Study On Ipv4 and Ipv6”,2013 International Conference on Communication System and Network Technology,2013 IEEE.

[3] R.A.K. Aljaafreh ,J.E. Mellor, M.A.Kamala ”Bi-Directional Mapping System as a New IPv4 /IPv6 Translation Mechanism”2008, IEEE

[4] J. Gnana Jayanthi , S. Albert Rabara,”IPv6 Addressing Architecture in IPv4 Network”,2010 Second International Conference on Communication Software and Networks,2010 IEEE.

[5] C. E. Caicedo,J.B.D,Joshi,S.R.Tuladhar,”IPv6 Security Challenges,” Computer ,Vol. 42,Issue 2,2009,pp. 36-42.

[6] H. Afifi, and L.Toutain:”Methods for IPv4-IPv6 Transition”, IEEE, 1999.

[7] E. Jankiewicz , D.Green,M.Fiuczynski,”IPv6 Translator For IPv4 Embedded Systems”,IEEE,2001.

Shian-Shyong Tseng , Jui Feng Weng , Li Lung Hu ,Hsu Nai-Wen” Ontology –based Anti-Threat Decision Support System For iPv4/IPv6,2014,IEEE