*I.J. Education and Management Engineering,* **2016, 1, 11-17**
Published Online January 2016 in MECS (http://www.mecs-press.net)
DOI: 10.5815/ijeme.2016.01.02

***Available online at http://www.mecs-press.net/ijeme***

# Active Networks: Applications and Security Issues

Azka

*BS Abdur Rahman University,Vandalur, Chennai,600048, India*

## Abstract

Active networks introduce a new concept to network architecture. Network nodes are capable of executing codes carried by packets which change their state. Active networks provide a flexible networking environment by their programming capabilities. Although active networks have benefitted networking largely, at the same time they pose many security threats due to their complexity. Since active networks have become famous because of programmability but it’s increasing flexible nature opens doors to new security risks. Currently research is being conducted to find out the benefits of active networks over the traditional networks and also to cope up with the security risks that active networks pose. The paper focuses on the benefits of active network over the passive network. The objectives and applications of active networks are briefly discussed. The methodologies of deploying active networks are also mentioned. In the latter part the security issues raised by active networks are presented and methods to cope up with them are also briefly discussed.

**Index Terms:** Active networks, passive networks, SANE, capsules, discrete approach of active networks.

## 1. Introduction

Keeping up and developing internet have become a tedious task.  More and more standards are being introduced which adds to the confusion owing to their complexities. In shared network scenario it’s hard to compound new technologies and the existing standards. Also new protocols are evolving at a slow pace.

Active network is a novel approach that can address above problems. Active networks provide the facility of making customized calculations on the packets flowing through the nodes. This is possible by adding an additional program fragment to the packet. Such packets are termed as ‘smart packets’ because they carry along the instructions that handle them through the network dynamically.

In contrast, traditional passive networks have each node functioning as per a fixed process or routing protocol. Such networks don't execute any code or program at any node.

Currently it is one of the most common types of network. The network architecture is pre-structured before it

* Corresponding author.
E-mail address:

starts sending packets. The network nodes are unable to execute any code. The static behaviour of the nodes is related to predefined network strategy or routing table entries, which are only updated manually or by neighboring routers.

## 2. Active v/s Passive Network

The passive network environments have hosts (senders and receivers) performing at the ends of the network architecture. These hosts perform computations up to the top most layer for accurate delivery and reception of packets. The network devices or routers are able to do calculations up to network layer.

The passive networks are rigid in nature since all the packets originating from sending nodes are treated in similar fashion.In active networks the intermediate routers are capable of performing computations up to the application layer and hence route the packets dynamically. Users can program the network by appending programs into them. The active networks are comparatively flexible since they carry smart packets i.e. the data packets with instructions injected into them which handle them across the network.

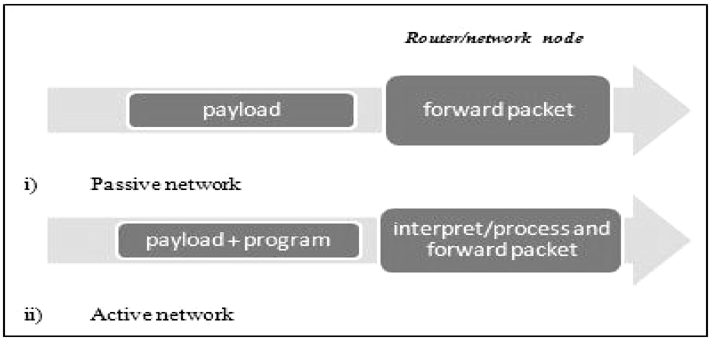

Fig.1. Passive v/s active data packet

## 3. Why Active Networks?

A lot of problems are being faced by assortment Internet technologies, some of which are mentioned below:

- The difficulty of introducing new technologies in the already existing network infrastructures.
- Repetition of operations at different layers of internet protocol.
- Evolving and implementing of new network services is a slow and expensive process.
- Recent Applications like firewall packet filtering, web proxies, multicast routers etc require computations to be performed within the network. These applications and lot of latest trends and developments have adopted a variety of ad hoc services for performing user-driven computations.

The concept Active Networks is naive, where a network is not just opaque carrier of data but a smart computational network. Active Networks consist of active nodes that dynamically control and modify the network behaviour by performing customized operations on the data flowing through them. Although traditional packet switched networks also do some minimal computations like header processing, and signalling etc but active networks in addition to computations on the data also enable users or third parties to create and tailor services to their particular applications and even to current network conditions by injecting programs into the network.

Active networks addresses above stated problems in following ways:

- By Active Networks deployment new services would be quick, bypassing the lengthy process of process since network nodes can be modified dynamically.
- Active networks are capable of reducing the time required to evolve and deploy new network services.
- Active networks offer a platform for experimenting with new network services and features on a realistic scale without interfering with the regular network services and thus reducing the cost of research and development in the field.
- Active networking could replace the numerous ad hoc approaches currently being used for network based computation by letting the users to program their networks.

Active network solutions could possibly lead to the development of new applications that were unimaginable with traditional networks and have addressed many issues faced by presence of variety of protocols and standards.

Active network system allows processing of these smart packets on network nodes by multiple ways. Since these programmable networks allow code from various different sources to be run on the network nodes, so they undoubtedly invite security threats too. Such security concerns can be dealt by making use of safe languages for writing programs for packets or nodes and by keeping execution restricted to certain environments.

## 4. Objectives of Active Networking

Active networking bypasses the lengthy standardization process of the operations of network nodes since it functions dynamically with the help of programmable open nodes. In this way active networks cut additional costs because standardization of new creative ideas of functions requires additional investments.

## 5. Applications of Active Networking

All the applications of active networks are by its ability to program the network. It is quite easy to deploy new and innovative services at intermediate network nodes.  This section highlights various applications which can be enhanced by virtue of active networking. E.g. network management, congestion control, multicasting, and caching.

### *5.1. Caching*

The caching is a suitable method of reducing response time and preventing congesting by minimizing traffic flow across the network. This scheme locates the frequently accessed objects to closer to the clients. This process requires deciding about the location of these objects and is being configured manually which makes is less capable in case of dynamic situations.

At each network node active networking can route cache requests and information about closer caches to cache locations.

### *5.2. Network Management*

Due increase in the number of network nodes and their added complexities, it is hard to manage the networks using traditional network control mechanisms. Network management stations are flooded with loads of information which can be redundant too reporting the state of packets being transferred. Active network deployment can address the above stated problems of network management quite simply. By the virtue of programmable nodes, each node can act as a network management station reducing the bandwidth consumption and delays which are currently faced by polling in network management. Since the packets in active networking scenario can carry executable code, special instructions can be appended in the packets which would be executed on encountering a problem in network and hence changes the network state dynamically. This approach reduces the implosion caused by current network management techniques.

### *5.3. Multicasting*

By programmable networks multicasting can also be affected in a positive way. The traditional multicasting approach does not reveal the network topology, number and position of receivers. This type of services proves to be good for unreliable transmission of data but poses problems for reliable transfer of packets and in recovering from loss of packets. Active networks can ensure reliable and robust service by including the number of receivers and their positions. In case of losses the retransmission can be done from nearest node using the network node caches thereby reducing delay.

### *5.4. Congestion Control*

Network congestion is a prime problem which impedes the smooth functioning of a network and it is unlikely to be solved in the near future. Whenever congestion like situation arises in a network, the user is informed about it after considerably a long period until the congestion signal propagates through the network so that he/she can manually fix it. From the point of first instance of congestion until it is fixed a good amount of time is elapsed which worsens the congestion.

With buffers in active nodes, these can constantly keep on checking the available bandwidth and can regulate the rate of packets flowing. In active network scenario changes in the rate of data flow can also be adjusted dynamically. Transferring of packets and selectively dropping of less important packets is also done efficiently by active network devices.

### *5.5. Quality of Service*

Network managing mechanisms that require the adjustments by the senders as per the network conditions have disadvantages like time required for detection of some glitch, reaction and resending. During this period the conditions can worsen and hence affect the network performance. If the information about the adaptations and adjustments to be made in the network (in case of occurrence abnormal conditions) are included in the network nodes, suitable adjustments can be made when needed by executing the appropriate code.

## 6. How to Build Active Networks?

There are two possible approaches to build active networks. A discrete or out-of-band approach and an Active networks or programmable networks can be configured by two possible distinct approaches, discrete or out of band approach and integrated or in-band approach depending on the way data and code are carried either separately or jointly.

### *6.1. Discrete Approach*

Discrete approach of active networking is also known as Programmable Node Approach. The code or instructions are kept separate from the payload data. The user sends the executable code to the node where it is stored and executed when required. In this approach active packets carry reference to code. Code is fetched from neighbor node or server, if not already present.

When data arrives at the node it is examined and appropriate program is executed related to the packet. This distinct transfer of data and program is desirable when careful control of program is required or when program is large and contains many instructions.

### *6.2. An Integrated Approach*

The Integrated Approach of active networking is termed as the Encapsulation Approach or Capsule. In this the program is appended with every data packet of data sent over the network which is jointly termed as capsule. In an extreme case of active programming, a capsule always contains executable code, be it just a single instruction even.

When such integrated packet arrives at an active node, it node examines it and forwards the appended data part depending on its interpretation of the program part of the program. The active nodes are equipped with a mechanism to interpret and execute the embedded program.

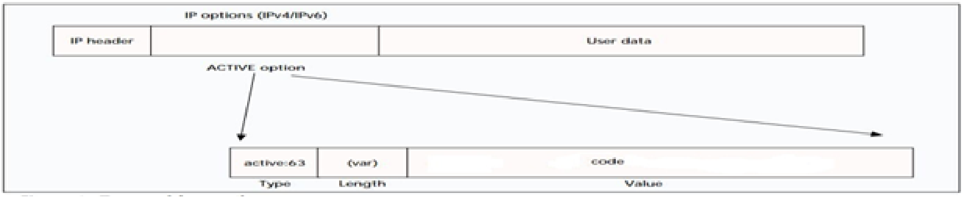

Fig.2. An active network capsule

Each capsule unit is identified using the framing mechanism of data link layer. The capsule is examined and program part is dispatched to a transient execution environment.

The active network administrator needs a programmable network Application Program Interface, some mechanism to inject code into packets over the network. An active network environment has fixed part and a variable part. The variable part has no restrictions in predicting the node behavior whereas the fixed part has predefined parameters and permits only slight variations from a standard behaviour. The fixed part makes it possible to understand the influence of single nodes on the whole behavior of the network, while the variable part depicts the case put to use currently. The optimum choice for smooth functioning of network would be somewhere in between the fixed and variable approaches.

## **7. Active Network Security**

Active networking poses many threats to security with user being able to program the network nodes. The security of a system lies in the extent of access to the resources and in an active networking environment managing the resources is complicated so securing the resources becomes difficult.

A secure network ensures privacy, integrity and availability of the data flowing through it. By safety we mean reducing the imminent threats by abnormal behavior of network or security attacks. In active networking a packet is injected with code that is capable of executing code and changing the status of network nodes (routers/switches). These nodes are essential resources and their proper functioning is required for correct behavior of the whole network system. Hence the execution environment needs to be strict in order to safeguard the resources from any malicious penetration.

In traditional networking the resources consumed by processing a packet at node are quite small compared to the cost of processing an active data packet. In the former the only resources consumed by a packet at a node are memory for temporary packet storage and CPU cycles required to route the packets. Even if option processing is also included, the CPU overhead would still be minimal. Hence in traditional networking environment strict resource control in the network nodes is not considered mandatory, only end to end security policies are enforced. Although this approach has worked efficiently in the past, denial-of -service attacks can easily prevail and it is difficult to ensure quality of service.

However active networks are less rigid due to programmability by users, hence active networks open doors for more security threats and safety issues that need to be addressed are tremendously increased.

Problems that are most likely to occur in an active networking environment are:

- An active packet can damage resources or services by modifying r erasing the contents of memory or a node may destroy an active packet.
- Since an active packet consuming more CPU cycles as compared to traditional technology, the node may not function properly and another active packet in queue won’t be cannot be able to access the resources and hence cannot be executed or forwarded.
- Critical or private information of a node is highly vulnerable in an active network environment. Besides an active packet if it contains private data is also vulnerable even if it is encrypted since it would need decryption before it’s executed.

The above security issues in active networks can be addressed by taking up following security measures

- If the time of execution and the number of nodes to be traversed by an active node is limited, the resources can be prevented from illegal use monopolizing the resources of a node.
- Authenticating any active packet can assure that the packet is from a valid user, although it doesn’t it’s harmlessness
- A security policy can be enforced which determines level of access to each resource. This method can effectively control the access of an active packet to each resource depending on its security level.

The above methods ensure security of nodes and prevent them from any modification by malicious active packets. The active packets carrying executable code are also vulnerable to losses; hence it becomes essential to protect them as well. We can safeguard active packets by encryption and fault tolerance mechanisms.

- Encryption renders the data and code unintelligible while packet is in transit. The packet can be deciphered only by sender and receiver. If the programs in active program are executed in encrypted format the security of active packets can be ensured.
- The fault tolerance aims at robustness of an active networking system which includes replication, persistence, and redirection.

A duplicate copy of each packet can be produced when required and packet can be temporarily stored if there is a crash or failure in the node. A packet can take an alternative route if the default route fails. Although replication and persistence are not acceptable in majority of network scenarios since it consumes memory and bandwidth but encryption and redirection are essential techniques that ensures security and robustness of an active networking system.

On its arrival, if the packet is not authenticated, then it may be allowed to execute the code in a restricted environment or its execution may be stopped.

## 8. Conclusions

Active network nodes are capable of executing code carried by the packets passing through them. Such networks provide dynamic handling of network services by modifying network behaviour at any time. Various applications where active networks can be beneficial have been highlighted like network management, quality of service, congestion control, caching and multicasting etc. The programmability of active networks affects its performance because of safety and security requirements. Although active networks have plenty of benefits but by ability to execute code, these pose many security threats and hence active networks have been limited to research environments. If effective research is done the programming paradigms of active networks then active networks can prove to be successful and would create a revolution since network nodes would not require the standardization and network protocols can be upgraded automatically.

## References

[1] Stanislav Shalunov et al., *"One Way Active Measurement Protocol"*, RFC 4656, September 2006.
[2] Hélder Veiga et al., "*Active traffic monitoring for heterogeneous environments*", 4th International Conference on Networking, ICN'05, April 17-21, 2005
[3] Federico Montesino-Pouzols, "*Comparative Analysis of Active Bandwidth Estimation Tools*", IPS-MoMe 2004
[4] Kasera S, Bhattacharyya S, Keaton M, Kiwior D, Zabele S, Kurose J and Towsley D, "*Scalable Fair Reliable Multicast Using Active Services*", IEEE Network Magazine, 14(1), 2000.
[5] D. S. Alexander, W. A. Arbaugh, M. Hicks, P. Kakkar, A. D. Keromytis, J. T. Moore, C. A. Gunter, S. M. Nettles, and J. M. Smith, "*The switchware active network architecture*," IEEE Network Magazine, special issue on Active and Programmable Networks, 1998.
[6] Liskov, B., et al.Safe and Efficient Sharing of Persistent Objects in Thor. in SIGMOD '96 1996.Montreal, Canada.
[7] Alex Galis, et al A Flexible IP Active Networks Architecture, Volume 1942 of the series Lecture Notes in Computer Science pp 1-15, 2001
[8] Kenneth L. Calvert, Samrat charjee and Ellen Zegura, Directions in Active Networks, IEEE Communications Magazine October 1998.

## Authors' Profiles

**Azka** (born June 8, 1989) is a Research Scholar in B S Abdur Rahman University Vandalur, Chennai -600048, India. Her field of interest is Networks and Security and she is pursuing research in security of Internet of Things.

**How to cite this paper:** Azka,"Active Networks: Applications and Security Issues", International Journal of Education and Management Engineering(IJEME), Vol.6, No.1, pp.11-17, 2016.DOI: 10.5815/ijeme.2016.01.02