Wired Network Security – Challenges for Researcher

Aiyeshabi S. Mulla
Dept. of Computer Applications,
Bharati Vidyapeeth Deemed University,
I.M.R.D.A., Sangli.

Riyajuddin Y. Mujawar
Dept. of Computer Applications,
Bharati Vidyapeeth Deemed University,
I.M.R.D.A., Sangli.

Abstract –
Network security has become more important to personal computer users, organizations, and the military. Thus Security is crucial to networks and applications. Although, network security is a critical requirement in emerging networks, there is a significant lack of security methods that can be easily implemented. Securing the network is just as important as securing the computers and encrypting the message. This paper focuses on the fuzzy based approach for various parameters of network security that will adjust the security measure and improve the security performance.
Keywords - Fuzzy logic, Network security, Security Measure, Security Performance.

1 INTRODUCTION

A Network security is a threat, intrusion, denial of service or other attack on a network infrastructure that analyzes and gain information to eventually cause network to crash or to become corrupted. The entire field of network security is vast and in an evolutionary stage. It consists of the provisions and policies adopted by the network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of the computer network and network-accessible resources. It covers public and private computer networks used in everyday jobs i.e. businesses, government agencies and individuals.

There exists a "communication gap" between the developers of security technology and developers of networks. Network design is a well-developed process that is based on the Open Systems Interconnections (OSI) model. The OSI model has several advantages when designing networks. It offers modularity, flexibility, ease-of-use, and standardization of protocols. The protocols of different layers can be easily combined to create stacks which allow modular development. The implementation of individual layers can be changed later without making other adjustments, allowing flexibility in development. In contrast to network design, secure network design is not a well-developed process. There isn't a methodology to manage the complexity of security requirements. Secure network design does not contain the same advantages as network design. Hence protecting network parameters is an important task to improve network security.

An essential factors which are termed as important keys for network security are:

- Identification
- Authentication
- Authorization
- Access Control
- Data Integrity
- Confidentiality
- Non-repudiation.

Identification means identifying authorized user, Authentication is for finding identity or origin of user or user name and password, Authorization gives access for using resources by authorized user, Access Control gives restricted to access data, Data Integrity ensures whether existing information complete and accurate & protect it from unauthorized modification, Confidentiality means protecting information from unauthorized disclosure.

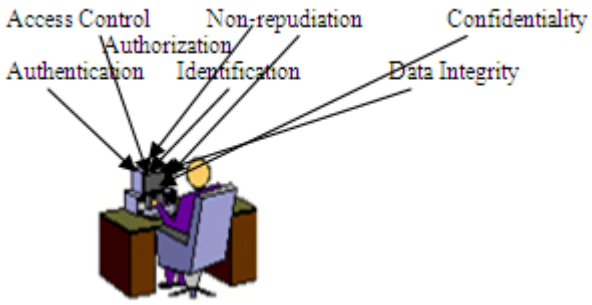

Fig.1 Secure User-Machine Interaction Hurdle Chain

While Communicating user has to go through specified hurdles for secure communication as shown in Fig.1.Mentioned parameters are important keys of network security otherwise system will suffer from its disadvantages like

- Intrusion
- Leak of information like hijack, access password, document etc.
- Unauthorized access
- Modification in data etc.[5]

Hence developing an effective network security plan understanding security issues, potential attackers, needed level of security and factors that make a network vulnerable to attack must be implemented.

I. NEED OF NETWORK SECURITY

Network Security includes two basic securities

- Information Security
- Computer Security.

Information Security protects data from unauthorized access and loss. Whereas Computer Security protects system from unwanted damages caused due to network like viruses, spywares, Trojan horse. The people who intentionally put such software on the network are called Hackers. Hence System needs

- Data link layer security
- Network layer security
- Transport layer security

Data link layer security includes link control. Network layer security includes routing of packets, packet scheduling. Transport layer security includes flow control. Hence Buffer management, Queue management, Routing, Load management are playing an important role in network security.

II. POLICIES AND OPERATIONS IN NETWORK SECURITY

Network Security Policy and Services should includes understanding of at which level of Network security to be established and maintained, what assets need to protect, what threats to what degree, identifying appropriate security policy elements for networks and meet the needs of network. Security Mechanisms includes security at various levels of layered architecture.

Network security operates in layers. It starts with firewall which controls network traffic. The
Next layers of security are antivirus programs on desktops and servers. Layers beyond that include password policies, data access permissions.

Following table shows seven layers of OSI model, their importance in security and which security mechanism should be applied for each layer for secure communication is mentioned.

TABLE I
OSI MODEL LAYERS & THEIR ROLE IN SECURITY MECHANISM

Layer No.	*OSI Layers*	*Security mechanism*
7	Application Layer	Identification, Authentication, QoS
6	Presentation Layer	Encryption Standards
5	Session Layer	Secure Password Policy
4	Transport Layer	Flow Control
3	Network Layer	Secure Routing, Congestion Control Policies, packet sequencing
2	Data Link Layer	Flow & Error Control
1	Physical Layer	Password management, topology

Network security is mostly contained within the physical layer. Cryptography occurs at Application layer. Authentication is performed on a layer above the physical layer.

For authentication, one may use one actor authentication, two-factor authentication or three-factor authentication. In one actor authentication, user uses username and password for authentication. In two-factor authentication, user uses something like security token or 'dongle' or an ATM card or a mobile phone. Where as in three-factor authentication, the user 'is' is also used like fingerprint or retinal scan. Network security in the physical layer requires failure detection, attack detection mechanisms, and intelligent countermeasure strategies.

III. TYPES OF ATTACKS AND SECURITY POLICIES IN WIRED NETWORK

A. Local Area Network

Wired LAN uses Ethernet cables and network adapters. Although two computers can be directly wired to each other using an Ethernet crossover cable, wired LANs generally require central devices like hubs, switches, or routers to accommodate more computers. Wired LANs offer superior performance. Wired LANs utilizing hubs can suffer performance slowdown if computers heavily utilize the network simultaneously.

Threats to a LAN environment [1] are-

- Unauthorized LAN
- Inappropriate access to LAN resources
- Disclosure of data
- Spoofing of LAN traffic
- Disruption of LAN functions

Unauthorized LAN includes poor password management for authentication, identification, known system holes. Inappropriate access to LAN resources is due to improper use of privilege mechanism for users, providing no access control for PC's on a file level basis. Disclosure of data is due to use of system default permission settings that are too permissive to users. Unauthorized Modification to data and software includes lack of a cryptographic checksum on sensitive data, lack of virus protection and detection tools. Disclosure of LAN traffic is due to lack of a cryptographic checksum on sensitive data. Spoofing of LAN traffic includes lack of a date/time stamp, lack of message authentication code mechanism or digital signature. Disruption of LAN functions includes inability to detect unusual traffic patterns (i.e. intentional flooding), inability to reroute traffic, handle hardware failures, unauthorized changes made to hardware components, improper physical security of LAN hardware.

1) Security policies for LAN

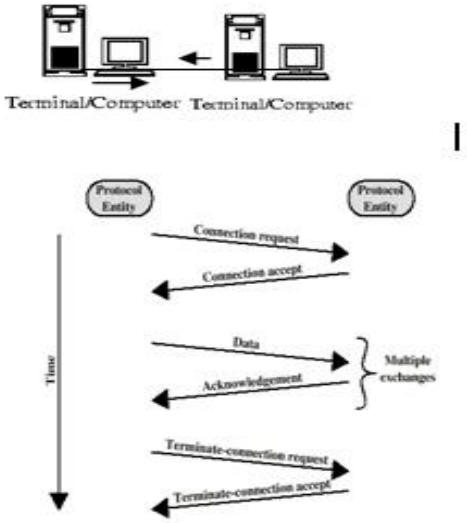

Fig. 2. Communication Methodology for Wired LAN

As shown in Fig.2 for communication, two ends must connect with each other with *handshaking* which is important to start communication. And then further communication will be proceeded. After finishing transmission established link must be disconnected.
To keep communication secure, polling, link control protocols plays an important role. Those protocols will work for buffering, routing, flow control mechanism etc.

Most factors affecting on LAN network performance are topology, load balancing, transmission media used for data transmission etc.

Hence for secure communication generally following mentioned precautions can be taken –

i. For identification and authentication, strong userid/password scheme, smartcards/smart tokens, biometrics based mechanism can be used.
ii. Restricted access to resources using grants or privileges.
iii. For data integrity various encryption technologies can be used.
iv. For logging and monitoring various LAN traffic management tools, auditing tools can be used.

2) Designing a Secure Local Area Network

To design and build a well-secured network topology, placement of hosts within the network, selection of hardware and software technologies, careful configuration of each component should be considered. Its flow is shown in Fig.3.

Here geographical arrangement, interconnection of hosts; used hardware and software, each components configuration matters largely in communication.

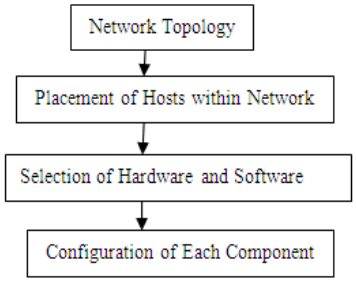

Fig.3.Secure Flow diagram for LAN

B. Telephone Network

Threats to the Public Switched Telephone Network are Service denial or disruption , unauthorized disclosure of sensitive information, Fraud, Masquerade, traffic analysis as shown in Fig.4. Due to such threats crosstalk communication, echo or other types of problems may arises.

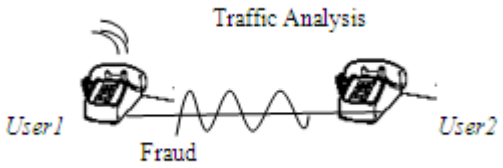

Fig.4. Threats in Telephone Network

1) Security policy in telephone network

Security policy in telephone network is achieved by using network monitoring tools. Internet Usage Monitor is used for monitoring telephone charges incurred during dial-up connections through dial-up modems.

IV. WHY FUZZY FOR NETWORK SECURITY?

Use of fuzzy logic in telecommunication systems and networks is recent and limited. Fundamentally, Zadeh's fuzzy set theory provides a robust mathematical framework for "real-world" imprecision and non-statistical uncertainty. Fuzzy logic-based approaches in network security can be used for -

Queuing : Queue stores IP packets with priority level inside routers or switches. Queue management algorithm[4] provide methods to determine order of sending data packets, control network transmission, solve congestion problem. Also it provides buffer management and packet scheduling.

Buffer Management[3] *:* It is at front of queue determining whether to drop packets or not. Its control scheme analyzed at 2 levels – data flow and data packet.

Distributed Access Control : Centralized approach has high security risk. Whereas decentralized approach provides authorization, flexibility, efficiency(n/w traffic minimized), enhanced security, resource sharing, better performance and reliability.

Load Management : Load balancing[9] is a technique to spread work between two or more computers, n/w links, CPU's, hard drives or other resources to get optimal resource utilization, throughput or response time. Using multiple components with load balancing instead of a single component increases reliability through redundancy.

Routing : Routing occurs at level 3 of OSI model. Routing determines optimal routing path through network. Routing algorithm stored in routers memory which affects on n/w performance.

Policing : Centralized policy management strategies regulate network and control traffic load for performance, efficiency and security. Various characteristics of effective policy based traffic and n/w management includes classification of n/w traffic (voice, data, audio, video) , degrees of control (rate, congestion level, bandwidth), stateful traffic inspection, user identification (IP address, hostname, login account), application identification (well known service), policy enforcement. Access control policy optimize use of shared resources.

Congestion Mitigation[6] **:** Due to inefficiency of buffer, packets may lost or overflowed. Hence implementation of connection-oriented protocols, such as TCP protocol watch for packet errors, losses, or delays in order to adjust the transmit speed.

Bandwidth Allocation : Bandwidth is the average rate of successful data transfer through a communication path. Bandwidth Allocation Protocol, along with its control protocol used to add and remove links in a multilink bundle over PPP, specifying which peer is responsible for making decisions regarding bandwidth management.

All above mentioned factors & their role for network are more important. Therefore, as present day complex networks are dynamic, hence there is great uncertainty associated with the input traffic and other environmental parameters, which subject to unexpected overloads, failures and also disobey accurate analytical modeling, hence fuzzy logic appears to be a promising approach to address many important aspects of networks.

V. CONCLUSION

According to the Fuzzy Logic Theory, everything is a matter of degree. Present day complex networks are dynamic, hence there is great uncertainty associated with the input traffic and other environmental parameters, which subject to unexpected overloads, failures and also disobey accurate analytical modeling. As Network security development system is a nonlinear task. Various parameters affecting on network security will slows down the performance of security. Hence use of fuzzy for this non linearity aspect will improves the performance of real time traffic and avoids the fragmentation problem.

VI. REFERENCES

[1] A. S. Sodiya, S. A. Onashoga, and B. A. Oladunjoye, "*Threat Modeling Using Fuzzy Logic Paradigm Issues*", in Informing Science and Information Technology Volume 4, 2007.

[2] Abbas Karimi, Faraneh Zarafshan, Adznan b. Jantan, A.R.
Ramli, M. Iqbal b.Saripan, "*A New Fuzzy Approach for Dynamic Load Balancing Algorithm*", *(IJCSIS)*

International Journal of Computer Science and Information Security, Vol. 6, No. 1, 2009

[3] *Amit Uppal, Yul Chu "An Efficient Buffer Management in a Network Interface Card*" IJCSNS International Journal of Computer Science and Network Security, VOL.6 No.7A, July 2006 .

[4] Bor-Sen Chen, Senior Member, IEEE, Sen-Chueh Peng, Member, IEEE, and Ku-Chen Wang, "*Traffic Modeling,Prediction, and Congestion Control for High-Speed Networks: A Fuzzy AR Approach*", IEEE TRANSACTIONS ON FUZZY SYSTEMS, VOL. 8, NO. 5, OCTOBER 2000.

[5] Chao-Hsien, "*Hacking Techniques in Wired Networks*".

[6] C. CHRYSOSTOMO, "*Congestion Control in Computer Networks using Fuzzy Logic*"

[7] Hua Jiang, "*Fuzzy Evaluation on Network Security Based on the New Algorithm of Membership Degree Transformation— M(1,2,3)*", JOURNAL OF NETWORKS, VOL. 4, NO. 5, JULY 2009.

[8] KEVIN BUTLER TONI FARLEY PATRICK MCDANIEL, "*A Survey of BGP Security* ".

[9] Ming-Chang Huang, S. Hossein Hosseini1 and K. Vairavan "*Load Balancing in Computer Networks"*

[10] Seyed Rasool Moosavi, "*Fuzzy based Design and tuning of distributed systems load balancing controller*"

[11] Tom Chothia, Dominic Duggan, Jan Vitek "*Type-Based Distributed Access Control*".

[12] Yuping Li, Jingyuan Yin, Guoqiang Wu, "*An Approach to Evaluating the Computer Network Security with Intuitionistic Fuzzy Information*", Advances in Information Sciences and Service Sciences, Volume3, Number7, August 2011.

[13] Zhang Lijuan Wang Qingxian, "*A Network Security Evaluation Method based on FUZZY and RST*", 2nd International Conference on Education Technology and Computer (ICETC), 2010.