IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661,p-ISSN: 2278-8727, Volume 16, Issue 6, Ver. II (Nov – Dec. 2014), PP 48-55
www.iosrjournals.org

An Advanced Intrusion Prevention Technique using MEDS

P. Rajapandian, Dr. K. Alagarsamy

Asst.Professor Dept of Computer Science Madurai Kamaraj University College Madurai, Tamil Nadu, India
Associate Professor Dept of Computer Application Madurai Kamaraj University, Madurai, Tamilnadu, India

Abstract:
Network security is a grouping of policy and necessities for make certain the protection of its possessions and the entire network interruption. It is evident in an execution of security rule and other computer network devices. The communication within the networks would deals with a range of hazards. Hence, the provision of protection system definitely needs within the communication channels. In existing scheme, the broadcasted information secured by many kind of Encryption Schemes and protect attacks by using Signature schemes to avoid intrusions during the transactions, but it may also leads in intrusion behaviors in some situation. Therefore, the priority based encoding encryption scheme is involved to prevent the intrusions within the channel allocation and in transactions using dynamic patterns. In some case, it may also cause security issues and make interruption in transactions, if any outflow of the encoding encryption patterns by the intruder. Thus, the objective of this paper is to construct a tough security strategy to prevent intrusions within the network transactions. In this paper, the Matrix Encoding and Decoding Scheme (MEDS) is included with the encryption scheme to build a hard-hitting intrusion protection system. This Scheme classifies the data packets in a matrix format and allows the encoding progression in a probabilistic manner to avoid the leakage of the security patterns.

I. Introduction

Computer network is collections of computing devices that are connected in assorted traditions in classify to commune and allocate resources. However, some connections are wireless, using radio waves or infrared signals. The generic term node or host refers to any device on a network. Data transfer rate: the speed with which data is moved from one place on a network to another. Data transfer rate is a key issue in computer networks. Computer networks have opened up an entire frontier in the world of computing called the client/server model. A machine and its software that serve as a special gateway to a network, protecting it from inappropriate access is known to be Firewall. Filters the network traffic that comes in, checking the validity of the messages as much as possible and perhaps denying some messages altogether and enforces an organization’s access control policy.

Network security is intentional attacks on computing resources and networks persist for a number of reasons. Complexity of computer software and newly emerging hardware and software combinations make computer and the network susceptible to intrusion. It is difficult to thoroughly test an application for all possible intrusions. There are several security threats occurs in the communication channel of the networks such as denial of service, an intermediary for another attacks, unprotected window shares, email spoofing, packets sniffing, etc. Many businesses rely heavily on computers to operate critical business processes. Individuals are using computers for tasks that required discretion. Advent of Internet has provided a physical path of entry for every computer connected to the Internet. An always connected broadband connection is always vulnerable in this case providing security requires action on two fronts, namely the management and the technical fronts respectively. The management aspect relates to organizational policies and behavior that would address security threats and issues. The technical aspect relates to the implementation of hardware and software to secure access to computing resources and the network.

Firewalls are used for controlling access to the computing resources. In general, it acts at the network level controlling network access to computing resources. Firewalls can be implemented in software as well as in hardware. Therefore another security technique with efficient manner is encryption. By encryption, the data can be made illegible to the intruder. It can be implemented at the network level as well as the client level. For example, locally stored data can be encrypted and the network traffic could equally well be encrypted. The main objectives of network security are:

- **Confidentiality**: only sender, intended receiver should “understand” message contents. Sender encrypts message, receiver decrypts message.
- **Authentication**: sender, receiver wants to confirm identity of each other.
- **Integrity**: sender, receiver wants to ensure messages are not altered without detection.
- **Access and Availability**: services must be accessible and available to users.

For instance, if sender transmits information through a communication channel, the channel allocation is allotted regarding the location and the communication structure of the sender and the receiver. The transmitted information is relocated through these channels to the receiver, but there may be some intrusions occur in that channel. The intruder may intercept, modify or delete the information. The intruder may also eavesdrop: intercept messages; actively insert messages into connection, impersonation: can fake (spoof) source address in packet (or any field in packet), hijacking: "take over" ongoing connection by removing sender or receiver, inserting himself in place, denial of service: prevent service from being used by others.

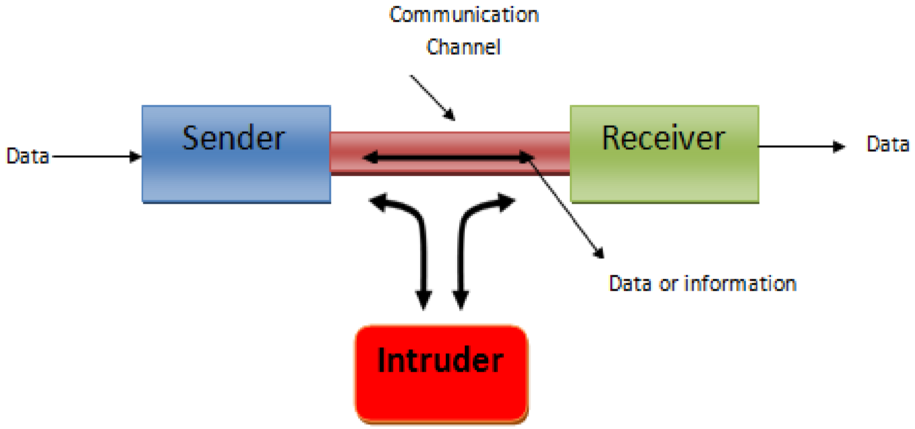


Figure: Intrusion assault

In the network, there would be various kinds of intrusions which occur during the transactions such as backdoor, email spoofing, etc. Protecting your network from intruders and attackers is to be effective, network security should be multilayered. You would protect your home from burglars by installing fencing at the property line (perimeter), putting locks on the doors and windows, installing a motion detector inside the house, and finally putting very valuable items in a safe concealed in the wall. Likewise, your network needs its own levels of protection: perimeter protection (a firewall) at the point it connects to the Internet, access controls (user accounts and permissions) to restrict access to data if someone does get into the network, and encryption of particularly sensitive data. A good firewall is your first line of defense, so ensure that the one you choose allows you to filter incoming data at more than one layer of the OSI networking model. Thus, the network needs a detection system known to be intrusion detection system (IDS). In many situations, the IDS may also cause issues in security constraints during transactions within the communication channels.

II. Dilemma of IDS

A block of address space not used by real machines and not pointed to by DNS entries. There is no legitimate reason to send packets to such addresses. Therefore, any host sending to such addresses is up to no good.

- Commonly used to detect scanning worms.
- Many organizations implement "auto-quarantine".
- This is especially common for university residence hall networks.
- Machines that do too much scanning are assumed to be virus-infected.
- They're moved to a separate net; the only sites they can contact are Windows Update, anti-virus companies, and the like honeypots and honeynets.
- Special-purpose host or network designed to be attacked.
- Equipped with copious monitoring
- Lure the attacker in deeper
- Waste the attacker's time; study the attacker's technique

IDS would detect bad things leaving your network and sensitive things leaving your network. Finds theft of inside information, either by attacker or by rogue insider and can be done in the network or in application gateways. Therefore, the IDS is not a complete solution for the intrusion attacks within the networks, thus the need of Intrusion Prevention System(IPS) would be introduced to defeat over the dilemma of IDS.

III. Intrusion Prevention System (IPS)

Intrusion prevention is a preemptive approach to network security used to identify potential threats and respond to them swiftly. Like an intrusion detection system (IDS), an intrusion prevention system (IPS) monitors network traffic. However, because an exploit may be carried out very quickly after the attacker gains access, intrusion prevention systems also have the ability to take immediate action, based on a set of rules established by the network administrator. For example, an IPS might drop a packet that it determines to be malicious and block all further traffic from that IP address or port. Legitimate traffic, meanwhile, should be forwarded to the recipient with no apparent disruption or delay of service.

IPS is a proactive protection technology that provides security at the network level. It is the first line of defense against malware. There is sometimes confusion between an IPS and a firewall. Personal firewalls are more basic, making allow/deny decisions to ensure that only "selected" programs are allowed to interact over the internet. Firewalls also block network communication on non-standard ports, which are generally not used by legitimate programs and services. On the other hand, an IPS goes one step further, and examines all network traffic that is allowed through the firewall. In order to avoid the performance degrading of the networks, the IPS must efforts as a proficient security component. Prevention system occupies quick because utilizes can happen. The prevention system would recognize and act in response exactly to avoid the intrusions. The key challenge in the network is the way bandwidth is allotted capably to introduce quality of service. This paper proposes a novel technique to make efficient security feature to the communication channel during transmission within the network. The key challenge is to prevent the intrusion which would affect the transmitted data. In the earlier sections, the information would be transmitted over the network with security constraints like encryption, digital-signature, providing keys, etc. There are several encryption algorithm are presented to encrypt the transmitted data.

In the past, Intrusion Prevention Systems simply protected against operating system (OS) threats or denial of service (DOS) and distributed denial of service (DDOS) attacks. These threats exploited vulnerabilities that were mostly in the OS network stack and services. Over the past few years, these OS components have become more robust. Thus the priority based encryption technique is included in the IPS. This priority based technique would introduce an adaptive encoded encryption scheme to protect data intrusion in the sound channel allocation known to be **Data Intrusion Protection Technique (DIPT)**. The transmitted packets are measured with some constraints to pertain the encoding and encryption to secure it. But the difference in this technique is the encoding pattern is generated randomly and dynamically based on those constraints. This would make a secure transaction in channel allocation. The major objective of this technique is to secure the encrypted data packets, because the intruder can distress the packets even it is encrypted. Thus, an adaptive scheme is introduced to secure the transactions by encoding with an encryption technique. This scheme would encode the information dynamically with dynamic patterns; therefore the intruder doesn't know the encoded pattern thus the information is secured within the communication channel. But there is an issue occurs in some situation would leads in outflow of the encoded pattern. The encoded pattern may leak in some case which would lend a hand to the intruder. Thus the objective is to make a hard-hitting security within the communication channels.

IV. IPS using Matrix Encoding and Decoding Scheme

Intrusion Detection Systems (IDSs) will be obsolete very soon (if they aren't already). In its place is something much more capable, an Intrusion Prevention System (IPS). IPSs are not a new technology; they are simply an evolved version of IDS. IPSs combine IDSs and improved firewall technologies, they make access control decisions based on application content, rather than IP address or ports as traditional firewalls had done. Because IDS and IPS technologies offer many of the same capabilities, administrators can usually disable prevention features in IPS products, causing them to function as IDSs. Intrusions: attempts to compromise the confidentiality, integrity, availability, or to bypass the security mechanisms of a computer system or network (illegal access). Intrusions have many causes, such as malware (worms, spyware, etc…), attackers gaining unauthorized access to systems from the Internet, and authorized users of systems who misuse their privileges or attempt to gain additional privileges for which they are not authorized. Although many intrusions are malicious in nature, many others are not; for example: a person might mistype the address of a computer and accidentally attempt to connect to a different system without authorization.

It's a dire fact that while every enterprise has a firewall, most still suffer from network security problems. IT professionals are acutely aware of the need for additional protective technologies, and network equipment vendors are anxious to fill in the gap. Intrusion Prevention Systems have been promoted as cost-effective ways to block malicious traffic, to detect and contain worm and virus threats, to serve as a network monitoring point, to assist in compliance requirements, and to act as a network sanitizing agent. IPS is primarily focused on:

- Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- Identifying problems with security policies
- Documenting existing threats
- Deterring individuals from violating security policies.

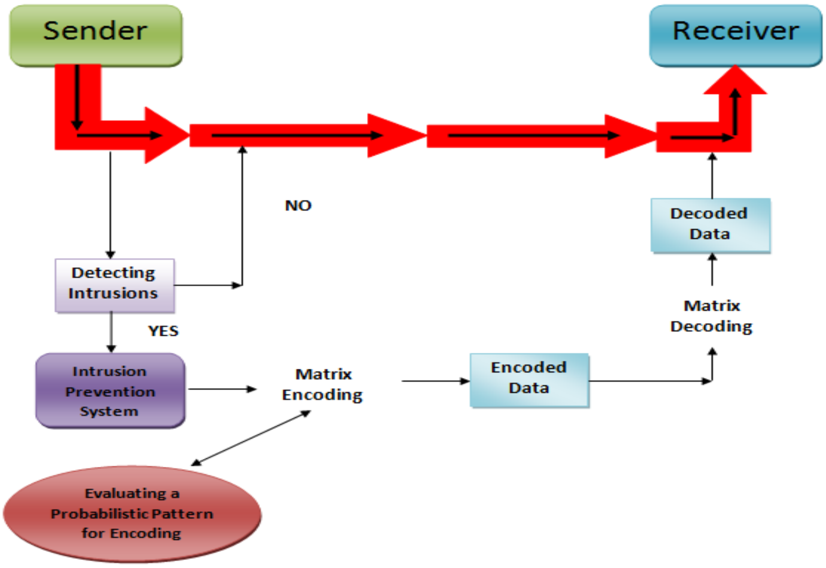
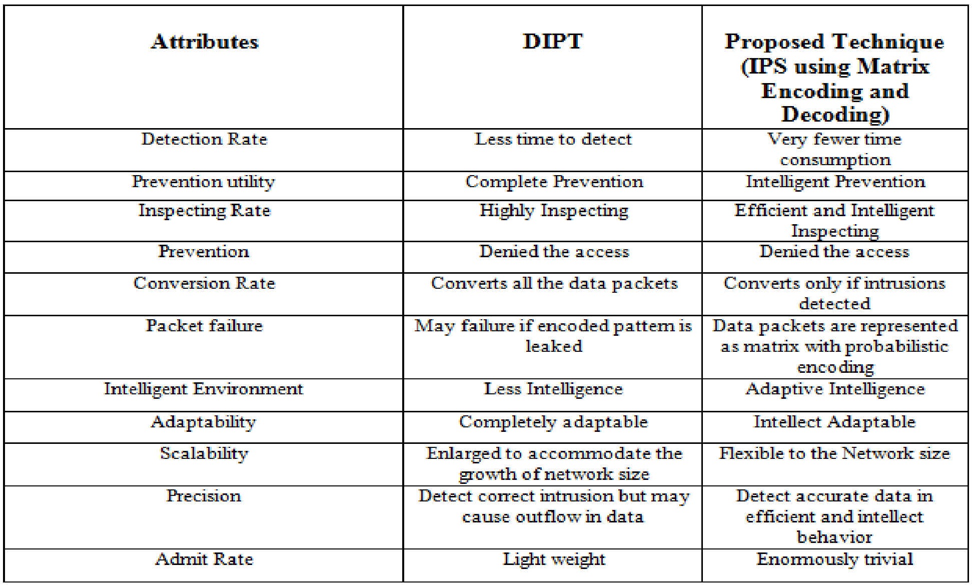


Figure: System Architecture

In addition, all types of IDPSs perform the following:

Recording information related to observed events. Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems. Notifying security administrators of important observed events. This notification, known as an alert, may take the form of audible signals, e-mails, pager notifications, or log entries. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information. Producing reports: Reports summarize the monitored events or provide details on particular events of interest. An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected. IPSs respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques. Terminate the network connection or user session that is being used for the attack. Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute. Block all access to the targeted host, service, application, or other resource.

The IPS could change the configuration of other security controls to disrupt an attack. Such as reconfiguring a network device to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities. Some IPS technologies can remove or replace malicious portions of an attack to make it benign. An example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient. For instance, an attacker could encode text characters in a particular way, knowing that the target understands the encoding and hoping that any monitoring IPSs do not. Most IPSs can overcome common evasion techniques by duplicating special processing performed by the targets. If the IPS can “see” the activity in the same way that the target would, then evasion techniques will generally be unsuccessful at hiding attacks.



Attributes	DIPT	Proposed Technique (IPS using Matrix Encoding and Decoding)
Detection Rate	Less time to detect	Very fewer time consumption
Prevention utility	Complete Prevention	Intelligent Prevention
Inspecting Rate	Highly Inspecting	Efficient and Intelligent Inspecting
Prevention	Denied the access	Denied the access
Conversion Rate	Converts all the data packets	Converts only if intrusions detected
Packet failure	May failure if encoded pattern is leaked	Data packets are represented as matrix with probabilistic encoding
Intelligent Environment	Less Intelligence	Adaptive Intelligence
Adaptability	Completely adaptable	Intellect Adaptable
Scalability	Enlarged to accommodate the growth of network size	Flexible to the Network size
Precision	Detect correct intrusion but may cause outflow in data	Detect accurate data in efficient and intellect behavior
Admit Rate	Light weight	Enormously trivial

Figure: Evaluation Analysis

In this context, **the matrix encoding and decoding scheme** is involved to make a complicated security in the sound channel allocation during communication. In this scheme, the patterns of encoding are allocated dynamically and probabilistic manner. Thus the intruder doesn't have any knowledge of the encoded patterns and the information is security from the intrusion vulnerabilities. Because the encoding technique is applied for the data packets, before that the data packets are represented as a matrix format. Then the matrix operations such as multiplication, addition, etc, would be applied to encode the data packets and also the key is generated in the matrix format. Then the encoding method is applied in the probabilistic manner like diagonally, row-wise or column-wise. Another important objective of this technique is the matrix encoding is applied regarding the convolution of the information. The complexity is measured in terms of data size and compactness of the information.

Matrix (plural matrices) is a rectangular table of elements (or entries).These elements are abstract quantities that can be added and multiplied with the Numbers. Matrices come in all possible rectangular shapes; the following are a number of examples of matrices.

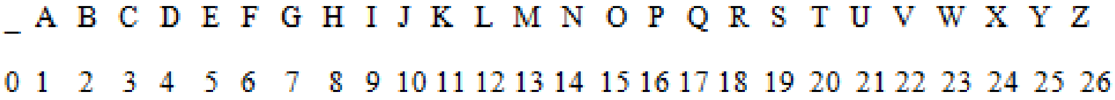
$$\begin{pmatrix} 1 & -1 & 0 & 4 \end{pmatrix} \qquad \begin{pmatrix} 2 \\ -3 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0 & 12 & -4 \\ 0 & 2 & 27 \end{pmatrix} \qquad \begin{pmatrix} 9 & -2 \\ 0 & 3 \\ 3 & 0 \\ -1 & 5 \end{pmatrix}$$

In general the matrix is denoted as:

$$\begin{pmatrix} a_{1,1} & a_{1,2} & \dots & a_{1,n} \\ a_{2,1} & a_{2,2} & \dots & a_{2,n} \\ \dots & & a_{i,j} & \\ a_{n,1} & a_{n,2} & \dots & a_{n,n} \end{pmatrix}$$

Each aij is called an element of the matrix (or an entry of the matrix); this denotes the element in row i and column j. The entries of the matrix are organized in horizontal rows and vertical columns. The size, or dimension, of the matrix is n x m, where, n is the number of rows of the matrix and m is the number of column of the matrix. Matrices are in several applications such as graph theory, linear combinations, computer graphics and cryptography. Cryptography is concerned with keeping communications private. Cryptography mainly consists of Encryption and Decryption. Encryption is the transformation of data into some unreadable form. Its purpose is to ensure privacy by keeping the information hidden from anyone for whom it is not intended, even those who can see the encrypted data. Decryption is the reverse of encryption. It is the transformation of encrypted data back into some intelligible form. Encryption and Decryption require the use of some secret information, usually referred to as a key. Depending on the encryption mechanism used, the same key might be used for both encryption and decryption, while for other mechanisms, the keys used for encryption and decryption might be different. One type of code, which is extremely difficult to break, makes use of a large matrix to encode a message. The receiver of the message decodes it using the inverse of the matrix. This first matrix, used by the sender is called the **encoding** matrix and its inverse is called the **decoding** matrix, which is used by the receiver.

The matrix encoding and decoding technique of the data packets are represented. Actually, two things happen in this step. First off, need to find a message worthy of undergoing this encryption. This may be difficult if just here because find secret codes, but have no secrets. The representation of the data packets in the matrix format is:



_	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26

Figure: Codes

Since we are using a 3 by 3 matrix, we break the enumerated message above into a sequence of 3 by 1 vectors:

$$\begin{bmatrix}16\\18\\5\end{bmatrix} \begin{bmatrix}16\\1\\18\end{bmatrix} \begin{bmatrix}5\\27\\20\end{bmatrix} \begin{bmatrix}15\\27\\14\end{bmatrix} \begin{bmatrix}5\\7\\15\end{bmatrix} \begin{bmatrix}20\\9\\1\end{bmatrix} \begin{bmatrix}20\\5\\27\end{bmatrix}$$

Note that it was necessary to add a space at the end of the message to complete the last vector. We encode the message by multiplying each of the above vectors by the encoding matrix. We represent above vectors as columns of a matrix and perform its matrix multiplication with the encoding matrix.

$$\begin{bmatrix}-3 & -3 & -4\\ 0 & 1 & 1\\ 4 & 3 & 4\end{bmatrix} \begin{bmatrix}16 & 16 & 5 & 15 & 5 & 20 & 20\\ 18 & 1 & 27 & 27 & 7 & 9 & 5\\ 5 & 18 & 20 & 14 & 15 & 1 & 27\end{bmatrix}$$

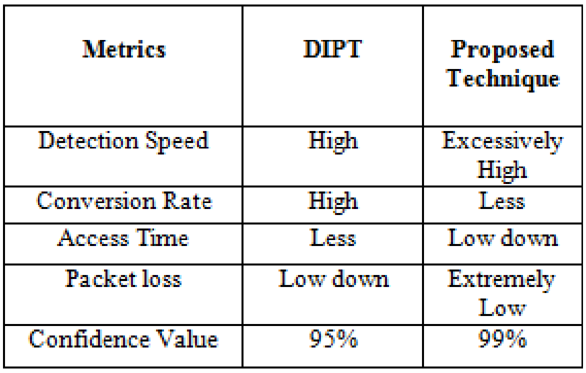
The message is transmitted in a linear form

$$\begin{array}{ccccccccc} -122, & 23, & 138, & -123, & 19, & 139, & -176, & 47, & 181, \\ -182, & 41, & 197, & -96, & 22, & 101, & -91, & 10, & 111, \\ -183 & 32 & 203. & & & & & & \end{array}$$

Finally, the intrusion prevention scheme is determined using Matrix encoding and decoding technique. The prevention and the security constraint using matrix scheme is involved only when the intrusion is detected. Thus it provides better results than the existing one. The time consumption in detecting and conversion is entirely reduced.

V. Performance Evaluation

This paper proposed an adaptive and efficient prevention technique for the sound channel communication system. To avoid and prevent the intrusions before it attack the information and make double layer authentication conception this paper gives a good performance results. The figure shows the detection ratio of intrusion for a particular time period gives better and quality of service then the existing services.



Metrics	**DIPT**	**Proposed Technique**
Detection Speed	High	Excessively High
Conversion Rate	High	Less
Access Time	Less	Low down
Packet loss	Low down	Extremely Low
Confidence Value	95%	99%

Figure: Performance assessment

The figure illustrates the confidence ratio among the existing DIPT and the proposed matrix scheme, there is some lack of confidence level is occurred. Then the features of detection time and conversion time are extremely efficient and intelligence in this proposed technique. At last, the accessing time and the failure of data packets are measured in this context; it predicts that the matrix scheme would provide the better performance.

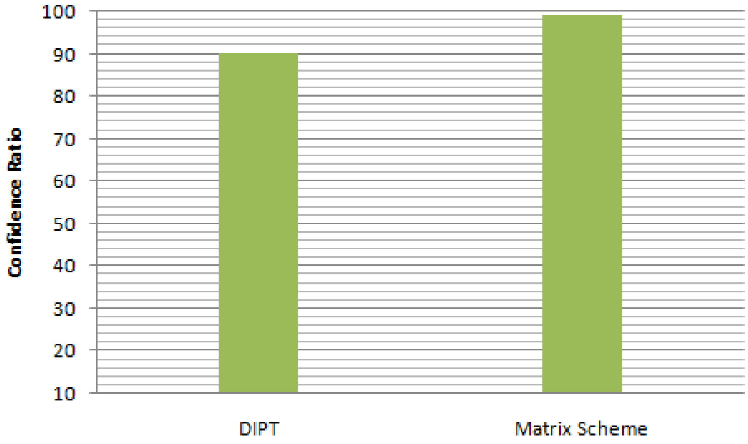


Figure: Confidence Ratio

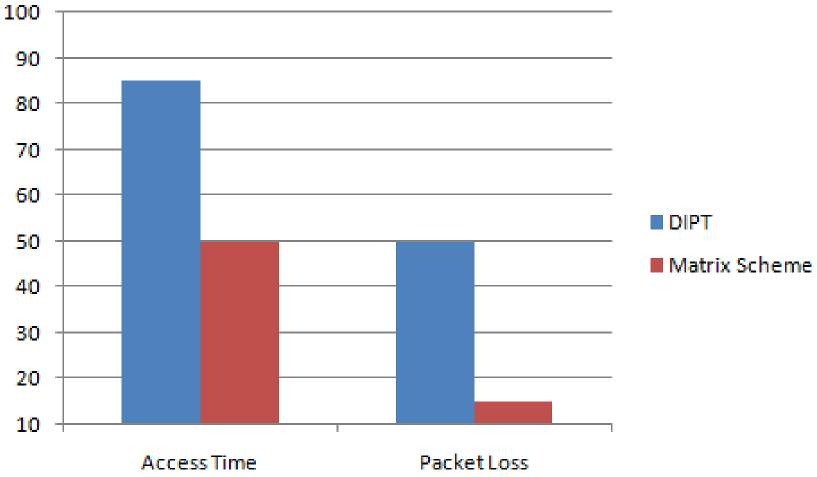


Figure: Access Time & Packet Failure

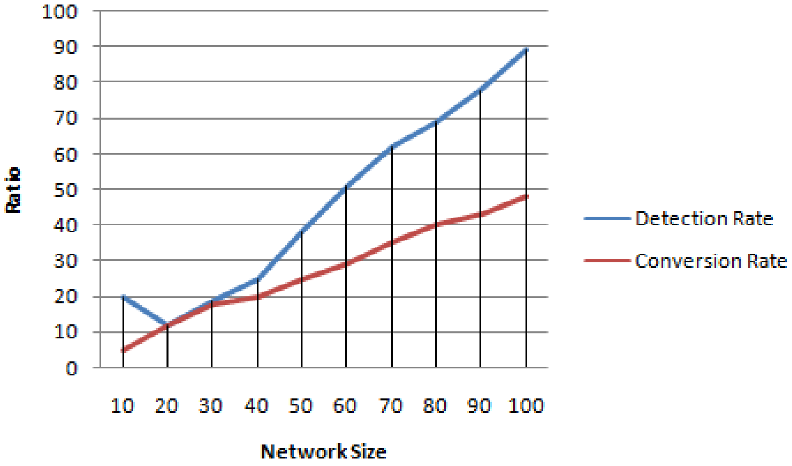


Figure: Evaluation

VI. Conclusion

Finally, this paper concluded that the security is key requirement of the communication system. In this paper we proposed, the new type of authentication is Matrix Encoding and decoding scheme. This approach is adaptive for all transaction during on networks and this mechanism flow providing services and giving recommendations. Encoding and Decoding is the method of putting a series of characters into an expert layout for proficient communication. We adapt our Efficient Encryption and Encoded method in this approach, Encoded and Encryption Needs Key value to Process, thus value generated based on the network transaction modes. This technique would entirely prevent the information from the intrusion even the encrypted packets of the information are attacked because; the double layer authentication is involved in this novel technique.

References

[1] Sumedha Kaushik and Ankur Singha, "Network Security Using Cryptographic Techniques", International Journal of Advanced Research in Computer Science and Software Engineering, Volume 2, Issue 12, 2012.

[2] Donald Graft, Mohnish Pabrai, Uday Pahrai, "Methodology for Network Security Design", IEEE Communications Magazine, 1990.

[3] Natarajan, S., Wolf, T., "Security issues in network virtualization for the future Internet", Computing, Networking and Communications, pp. 537 – 543, 2012.

[4] Yang Xiao, Chaitanya Bandela, Xiaojiang Du, Yi Pan, "Security mechanisms, attacks and security enhancements for the IEEE 802.11 WLANs", International Journal of Wireless and Mobile Computing, Vol. 1, Nos. 3/4, 2006

[5] Paula, F.S.,de Castro, L.N. ; Geus, P.L., "An intrusion detection system using ideas from the immune system", Evolutionary Computation, 2004. CEC2004. Congress, Vol.1, pp. 1059 – 1066, 2004.

[6] Raghunath, B.R.; Mahadeo, S.N., "Network Intrusion Detection System (NIDS)", Emerging Trends in Engineering and Technology, 2008. ICETET '08. First International Conference, pp. 1272 – 1277, 2008.

[7] Weiming Hu, "Network-based intrusion detection using Adaboost algorithm", Web Intelligence, 2005. Proceedings. The 2005 IEEE/WIC/ACM International Conference, pp. 712 – 717, 2005.

[8] Chai Wenguang, Tan Chunhui ; Duan Yuting, "Research of Intelligent Intrusion Detection System Based on Web Data Mining Technology", Business Intelligence and Financial Engineering (BIFE), pp.14-17, 2011.

[9] T. Ghorbani, A.A., Lu, W., Network Intrusion Detection and Prevention : Concepts and Technique, Springer, 2009.

[10] Stiawan, D.,Abdullah, A.H. ; Idris, M.Y., "The trends of Intrusion Prevention System network", Education Technology and Computer (ICETC), vol.1, pp. V4-217 - V4-221, 2010.

[11] Xinyou Zhang, Chengzhong Li ; Wenbin Zheng, "Intrusion prevention system design", Computer and Information Technology, pp. 386 – 390, 2004.

[12] Jain, P., Goyal, S., "An Adaptive Intrusion Prevention System Based on Immunity", Advances in Computing, Control, & Telecommunication Technologies, pp. 759 – 763, 2009.

[13] Deris Stiawan Abdul Hanan Abdullah Mohd. Yazid Idris, "Characterizing Network Intrusion Prevention System", International Journal of Computer Applications, 2011.

[14] G. Ollmann, "Intrusion Prevention Systems (IPS) destined to replace legacy routers," Network Security, vol. 11, 2003, pp. 18-19.

[15] D. Stiawan, A.H. Abdullah, and M.Y. Idris, "The Trends of Intrusion Prevention System Network," IEEE, ICETC 2010, vol. 4, 2010, pp. 217-221.

[16] T. Abbes, A. Bouhoula, M. Rusinowitch, and L. Inria-lorraine, "A Traffic Classification Algorithm for Intrusion Detection," IEEE 21st International Conference on Advanced Information Networking and Application Workshops (AINAW'07), 2007, pp. 0-5.

[17] Min Wu , Vetro, A. ; Yedidia, Jonathan S. ; Huifang Sun, "A study of encoding and decoding techniques for syndrome-based video coding", Circuits and Systems, 2005. ISCAS, pp.3527 - 3530 Vol. 4

[18] Al Haija, A.A, Mai Vu, "Analysis of encoding and decoding techniques for the interference channel with destination cooperation", Information Sciences and Systems (CISS), pp.1-6, 2013.

[19] Mamidi, S.,Schulte, M.J. ; Iancu, D. ; Iancu, A., "Instruction set extensions for Reed-Solomon encoding and decoding", Application-Specific Systems, Architecture Processors, pp. 364 – 369, 2005.

[20] Liyi Xiao, Zheng Sun ; Ming Zhu, "Efficient encoding and decoding algorithm used in Reed-Solomon codes for multiple fault-tolerance memories", Cross Strait Quad-Regional Radio Science and Wireless Technology Conference, vol 1, pp. 1569 – 1572, 2011.

[21] P.Rajapandian and Dr. K. Alagarsamy, "Intrusion Detection in DOS Attacks", International Journal of Computer Applications, Vol 15, No 8, pp. 33-37, 2011

[22] P.Rajapandian and Dr. K. Alagarsamy, "Secure Sound Channel Allocation using Data Intrusion Protection Technique", International Journal of Computer Technology and Applications, Vol 5, No 4, pp. 1477-1484, 2014