Discovery of Malicious Attacks to Improve Mobile Collaborative Learning (MCL)

Abdul Razaque and Khaled Elleithy

Department of Computer Science and Engineering, University of Bridgeport, Bridgeport, CT 06604, USA

`arazaque@bridgeport.edu,elleithy@bridgeport.edu`

Abstract

Mobile collaborative learning (MCL) is highly acknowledged and focusing paradigm in eductional institutions and several organizations across the world. It exhibits intellectual synergy of various combined minds to handle the problem and stimulate the social activity of mutual understanding. To improve and foster the baseline of MCL, several supporting architectures, frameworks including number of the mobile applications have been introduced.

Limited research was reported that particularly focuses to enhance the security of those pardigms and provide secure MCL to users. The paper handles the issue of rogue DHCP server that affects and disrupts the network resources during the MCL. The rogue DHCP is unauthorized server that releases the incorrect IP address to users and sniffs the traffic illegally. The contribution specially provides the privacy to users and enhances the security aspects of mobile supported collaborative framework (MSCF). The paper introduces multi-frame signature-cum anomaly-based intrusion detection systems (MSAIDS) supported with novel algorithms through addition of new rules in IDS and mathematcal model. The major target of contribution is to detect the malicious attacks and blocks the illegal activities of rogue DHCP server. This innovative security mechanism reinforces the confidence of users, protects network from illicit intervention and restore the privacy of users. Finally, the paper validates the idea through simulation and compares the findings with other existing techniques.

General Terms: Design*,* Development*,* Theory.

Index Terms

Client, DHCP server, rogue DHCP server, mobile learning environment, algorithms, signature-cum anomaly based Intrusion detection. Inclusion of IDS rules, sniffer, nikito, stick.

1. Introduction

The rapid developments in information technologies (IT) have improvised the use of mobile devices in open, large scale and heterogeneous environments.

The mobile devices provide the bridge to connect learners with institutions directly. This highly emerged platform has put the concrete foundation of MCL to corroborate pedagogical activities. The deployment of mobile devices has not only underpinned MCL but also created many chances for malicious attackers to crack the integrity and privacy of users. The mobile users are highly dependent on DHCP server for issuance of IP addresses.

The DHCP server provides highly organized and useful administrative service to mobile devices. However, unauthorized and misconfigured DHCP server (rogue DHCP) is used into a network; it creates the problems for users, breaking the security. It invites the intruders and attackers to redirect & intercept network traffic of any device that uses the DHCP. Attacker (The man-in-middle) modifies the original contents of communication. The malware and Trojans horse install rogue DHCP server automatically on network and affect the legitimate servers.

If the rogue DHCP server assigns an incorrect IP address faster than original DHCP server, it causes the potentially black hole for users. To control the malicious attacks and avoiding the network blockage, the network administrators put their efforts to guarantee the components of server, using various tools. The graphical user interface (GUI) tool is used to prevent the attack of rogue detection [5]. Idea of using multilayer swiches may be configured to control the attacks of rogue DHCP server but it is little bit complex and not efficient to detect rogue DHCP server and its malicious consequences [7] & [8].

Time-tested, DHCP Find Roadkil.net's, DHCP Sentry, Dhcploc.exe and DHCP-probe provide the solution to detect and defend rogue DHCP server malware [6]. All of these tools cannot detect the new malicious attacks.

Intrusion detection systems (IDS) are also introduced to ensure the protection of systems and networks. However, IDS cannot detect the intrusion due to increase in size of networks. The Signature based detection does not have capacity to compare each packet with each signature in database [2].

Distributed Intrusion Detection System (DIDS) is another technique to support the mobile agents. This technique helps the system to sense the intrusion from incoming and outgoing traffics to detect the known attacks [1]. Ant colony optimization (ACO) based distributed intrusion detection system is introduced to detect intrusions in the distributed environments. It detects the visible activities of attackers and identifies the attack of false alarm rate [3].

Anomaly based intrusion detection are introduced to detect those attacks for which no signatures exist [4], [6], [10].Both signature based and anomaly based IDS have not been used to detect the problems of rogue DHCP server. This paper introduces the multi-frame signature-cum anomaly based intrusion detection system supported with novel algorithms, inclusion of new rules in IDS and mathematical model to detect the malicious attacks and increase the privacy and confidentiality of users in MCL environment.

2. Related work

The modern technologies and its deployment in computer and mobile devices have not only created new opportunities for better services but from other perspective, privacy of the users is highly questionable. The network-intruder and virus contagion extremely affect the computer systems and its counterparts. They also alter the top confidential data.

Handling these issues and restoring the security of systems, IDS are introduced to control malicious attackers. IDS are erroneous and not providing the persistent solution in its current shape. The first contribution in the field of intrusion detection was deliberated by J.P Anderson in [28]. He introduced notion about the security of computer systems and related threats. Initially, he discovered three attacks that are misfeasors, external penetrations and internal penetrations.

The classification of typical IDS is discussed in [17]. The focus of the contribution is about reviewing the agent-based IDS for mobile devices. They have stated the problems and strength of each category of classification and suggested the methods to improve the performance of mobile agent for IDS design.

Four types of attacks are discussed in [21] for security of network. They have also simulated the behavior of these attacks by using simulation of ns2. A multi-ant colonies technique is proposed in [25] for clustering the data. It involves independent, parallel ant colonies and a queen ant agent. They state that each process for ant colony takes dissimilar forms of ants at moving speed. They have generated various clustering results by using ant-based clustering algorithm. The findings show that outlier's lowest strategy for choosing the recent data set has the better performance. The contribution covers the clustering-based approach.

The discussed work in [23], implements the genetic algorithm (GA) with IDS to prevent the network from the attack of intruders. The focus of technique is to use information theory to scrutinize the traffic and thus decrease the complexity. They have used linear structure rules to categorize the activities of network into abnormal and normal behaviors.

The work done in [18] is about the framework of distributed Intrusion Detection System that supports mobile agents. The focus of work is to sense the both outside and inside network division. The mobile-agents control remote sniffer, data and known attacks. They have used data mining method for detection and data analysis. Dynamic Multi-Layer Signature based (DMSIDS) is proposed in [2]. It detects looming threats by using mobile agents. Authors have introduced small and well-organized multiple databases. The small signature-based databases are also updated at the same time regularly.

Algorithm is presented for adaptive network intrusion detection (ANID). The base of algorithm is on naive decision tree and naive Bayesian classifier [19]. The algorithm performs detection and keeps the track of false positive at balanced level for various types of network attacks. It also handles some problems of data mining such as dealing with lost attribute values, controlling continuous attributes and lessening the noise in training data. Work is tested by using KDD99 benchmark for intrusion detection dataset. The experiment has reduced the false positive by using limited resources.

Moreover, all of the proposed techniques cover general idea of network detection but proposed MSAIDS technique handles the irreplaceable issues of DHCP rogue server. It controls signature and anomaly based attacks to be generated by DHCP rogue. The contribution also prevents almost all types of attacks. The major contribution of work is to validate the technique by employing innovative algorithms, inclusion of new rules in tradition IDS and mathematical model. It also helps the legitimate users to start secure and reliable MCL frequently. One of the most promising aspects of this research is uniqueness because there is no single contribution is available in survey about the DHCP rogue and its severe targeted attacks.

3. Possible Attacks of Rogue DHCP Server (SCENARIO-I)

With deployment of latest technologies, the need for automated tools has been increased to protect the information stored either on computers or flowing on networks. The generic idea to protect the data and thwart the malicious attackers is computer security. The introduction of distributed system has highly affected the security [11].

There are several forms of vulnerabilities and vigorous threats to expose the security of the systems. To take important security measures and enhancing the secure needs for organizations,

several mechanisms are implemented but those mechanisms also invite the attackers to play with privacy and confidentiality of users. One of the major threats for privacy of data is intervention of rogue DHCP server.

The first sign of problem associated with rogue DHCP server is discontinuation of network service. The static and portable devices start experiencing due to network issues. The issues are started by assigning the wrong IP address to requested clients to initiate the session. The malicious attackers take the advantages of rogue DHCP server and sniff the traffic sent by legitimate users.

Rogue DHCP server spreads the wrong network parameters that create the bridge for attackers to expose the confidentiality and privacy. Trojans like DNS-changing installs the rogue DHCP server and pollutes the network. It provides the chance to attackers to use the compromised resources on the network.Rogue DHCP server creates several problems to expose the privacy of legitimate users. The most three important attacks are shown in figure 1.
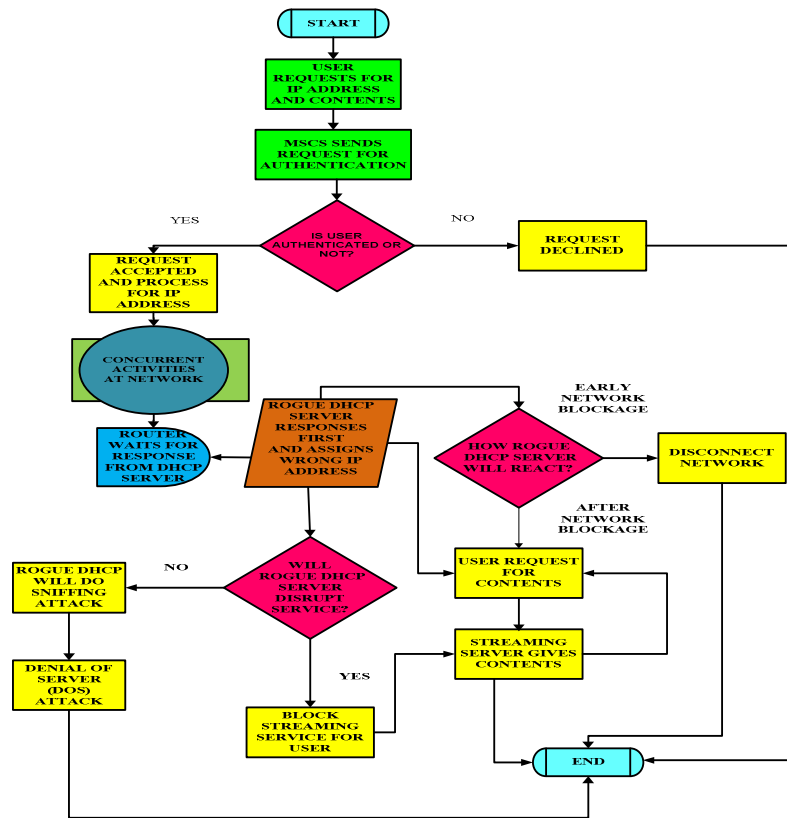

Fig. 1. Behavior of DHCP Rogue during the attack

3.1. Network disrupting attack

Rogue DHCP server makes the vague situation for legitimate DHCP server by sending many requests for issuance of IPs. This situation exhausts the pool of IP addresses of DHCP server, resulting it does not entertain the requests of clients for lease of new IPs. When process of issuance of IPs is blocked then rogue DHCP server appears in network as replacement of legitimate DHCP server. The rogue DHCP server releases the wrong network settings and in consequence causes the network disruption.

The DHCP server responds faster than corporate server on local area network for release of IP addresses. Rogue DHCP server continuously monitors the behavior of DHCP server and whenever any request comes through router for release of IP address, it issues the wrong IP address faster than legitimate DHCP server. Router does not have capability to detect issued IP address from rogue DHCP server. Once it issues its wrong IP address then continuously disrupts the network. Several mechanisms are introduced such as network access control (NAC) and network access protection (NAP) to force all the connected devices to be responsible for authentication to network.

The devices which do not meet the criteria of authentication are segmented on subnet or virtual Local area network (VLAN). All of these methods are challenging and difficult to deploy to protect the network disruption from attack of rogue DHCP server. To employ these mechanism, DHCP snooping must be implemented on switches otherwise users will not be able to obtain the information but from other side NAC and NAP are limited with some specific operating systems. These techniques are not efficient to control the attack rogue DHCP server.

It takes the control of whole network and also continues the connecting and disconnecting process at different intervals. The figure 2 shows the attacking process of DHCP rogue server and disruption of network.
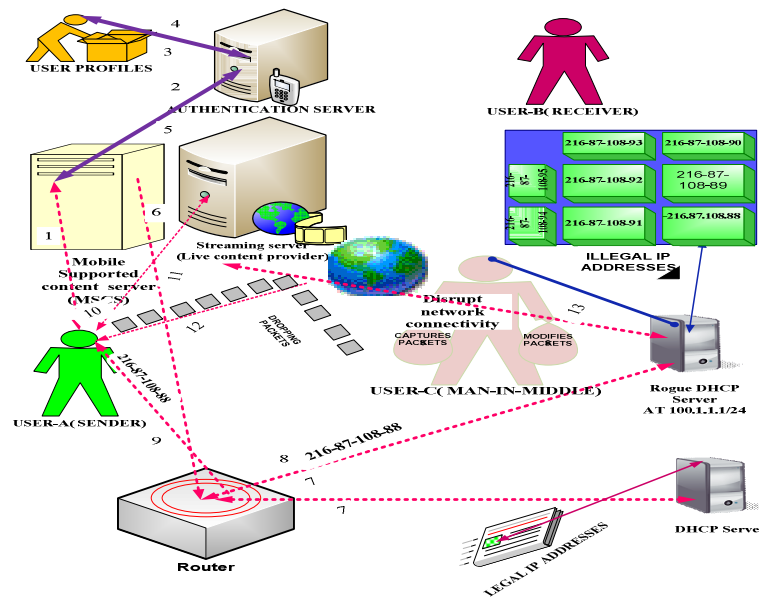
Fig. 2. Network disrupting attacking process

3.2. Sniffing The Network Traffic

It is brutal irony in information security that the features which are used to protect the static and portable devices to function in efficient and smooth manner; and from other side same features maximize the chances for attackers to compromise and exploit the same tools and networks.

Hence packet sniffing is used to monitor network traffic to prevent the network from bottleneck and make an efficient data transmission. Attackers use the same resources for collecting information for illegal use. Rogue DHCP server substantiates those malicious attackers to expose the privacy of users. When networks are victim of rogue DHCP servers that provide very important information related to IP address, domain name system and default gateway to attackers.

25

Rogue DHCP server sets default gateway as IP address of malicious attacker's proxy. In this case, attacker can sniff the traffic and wreak the privacy of users shown in figure 3.
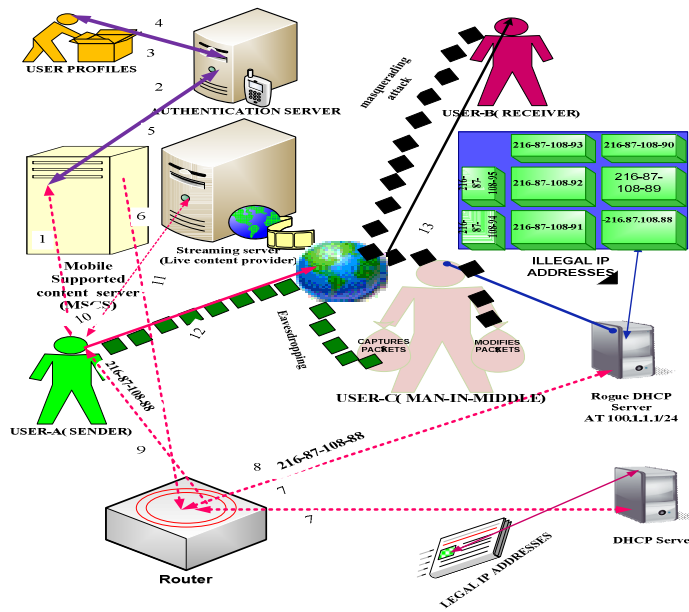

Fig. 3. Sniffing the traffic and masquerading attack

Rogue DHCP server also helps the intruders to capture the MAC address of legitimate users. It causes the sniffing the traffic through switch. In this case, attackers spoof the IP addresses of both sender and receiver and play the man-of-middle to sniff the traffic and extract important contents of communication.

3.3. Denial of service attack (DOS)

Intruders that get support through rogue DHCP server also use DOS attacks after sniffing the confidential contents of traffic. Due to DOS attack, the access of important services for legitimate users is blocked. Intruders often crash the routers, host, servers and other computer entity by sending overwhelming amount of traffic on the network.

Rogue DHCP server creates friendly environment for intruders to launch DOS attacks because intruders need small effort for this kind of attack and it is also difficult to detect and attack back to intruders. In addition, it is also easy to create the floods on internet because it is comprised of limited resources including processing power, bandwidth and storage capabilities. Rogue DHCP can make flooding attack at the domain name system (DNS) because target of intruders is to prevent the legitimate users from resolving resource pertaining to zone under attack [12] [13] & [16].

These attacks on DNS have obtained varying success while disturbing resolution of names related to the targeted zone. Rogue DHCP server can take advantages of inevitable human errors during installation, configuration and developing the software. It creates several types of DOS attack documented in literature [20]. [22] & [24]. Intruders with support of Rogue DHCP server make three types of fraggle or smurf, SYN Flood and DNS Attacks DOS attacks shown in figure 4. These attacks are vulnerable and dangerous for security point of view.
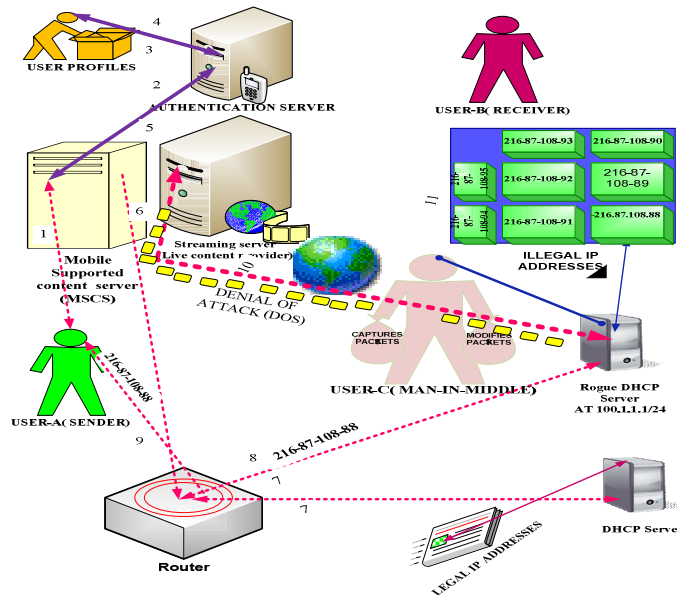
Fig. 4. Denial of service attack (DOS) attack

4. Proposed Solution (Multi- Fram Signature- Cum –Anomaly Based Intrusion Detection System)

Networks are being converged rapidly and thousands of heterogeneous devices are connected. The devices integrated in large networks, communicate through several types of protocols and technologies. This large scale heterogeneous environment invites the intruders to expose the security of users. Hence, IDS are introduced to recognize the patterns of attacks, if they are not fixed strategically, many attackers cross the IDS by traversing alternate route in network.

Many signature-based IDS are available to detect the attacks but some of new attacks cannot be identified and controlled. Anomaly-based IDS is another option but it can only detect new patterns of attack. The multi-frame signature-cum anomaly-based intrusion detection system (MSAIDS) supported with algorithms is proposed to resolve the issue of DHCP rogue. The proposed framework consists of detecting server that controls IDS and its related three units: (i) DHCP verifier unit (ii) signature database and (iii) anomaly database. During each detection process, intrusion detection starts matching from DHCP verifier, if any malicious activity is detected that stops the process otherwise checks other two units until finds whether activity is malicious or not. Figure 5 shows the MSAIDS.
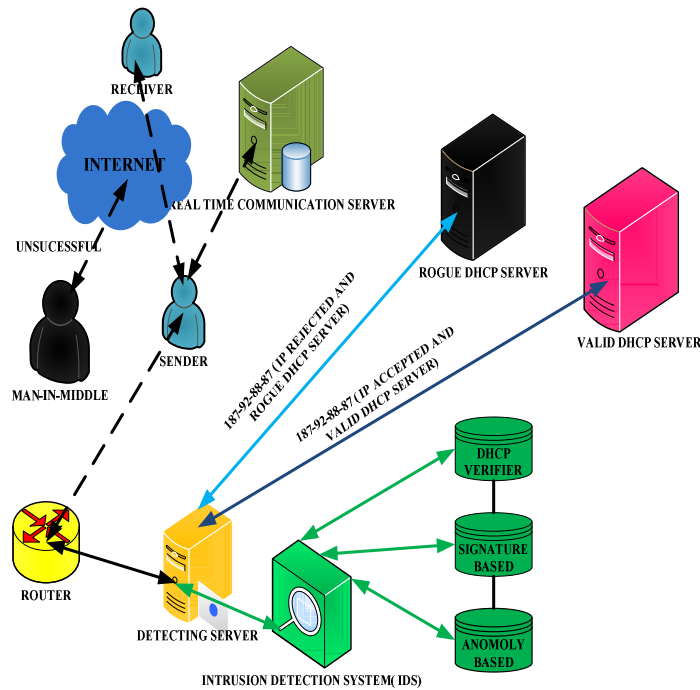
Fig. 5. Multi-frame signature-cum-anomaly based IDS

The detecting server (DS) is responsible to check the inbound and outbound traffic for issuance of IP address. The DS gets IP request (inbound traffic) through routers and forwards to DHCP server after satisfactory checkup. When any IP address is released for requested node then applies DHCP detecting algorithm for validation of DHCP server and detecting the types of attack shown in algorithm 1.

Algorithm 1: Verify DHCP server and detecting the attack

1. Input: MF =(FD, FS,FA & I)
2. Output : For every strategy I € FA, I € FS, D € FD)
3. D = Each valid DHCP Server
4. IP= Internet protocol address
5. N= Number of mobile devices
6. FD= Frame DHCP server
7. If D € FD
8. IP→ N
9. endif
10. S= Number of available signatures in signature based IDS (SIDS)
11. FS= Frame of signatures
12. FS ⊆ SIDS
13. I= Number & Types of attacks
14. For (I=S; I ≤ FS; I++)
15. If I ⊆ FS
16. SIDS attack alert
17. endif
18. endfor
19. A= Number of signatures available in Anomaly based Intrusion detection system AIDS
20. FA= Frame of AIDS
21. FA ⊆ AIDS

22. For (I =A; I ≤ FA ; I ++)
23. If I € FA
24. AIDS raises alert
25. If (I ∉ FS & I ∉ FA)
26.   No alert (No attack)
27. endif
28. endif
29. endfor

4.1. Central IDS

The aim of central IDS is to control and store messages received from DS. It works as middleware for DS and other layers to send the verification request and receive the alerts. The main function of central IDS is to update and manage the policy according to attack. If it needs any change in attack detection that is employed on all the layers. The central IDS implements the updated policy is shown in figure no 6.
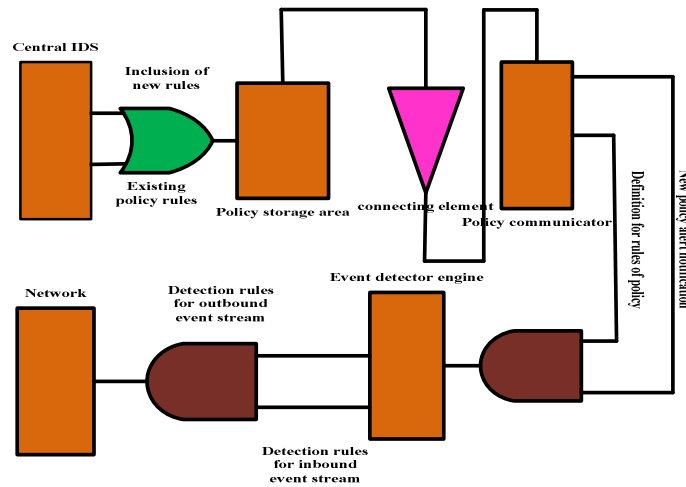

Fig. 6. Policy of Central IDS for network

4.2. DHCP Verifier

 DHCP verifier is the top layer that distinguishes between rogue DHCP and original DHCP server. The signatures of original DHCP servers are stored at the DHCP verifier. It checks the validity of the DHCP server that issues IP address for client. On the basis of stored signatures, DHCP server is identified whether it is rogue or original DHCP server.

Top layer produces the unique alert sign for both DHCP rogue and original DHCP. Top layer receives the parameters for verification from central IDS. DHCP verifier running on top layer is also responsible to return the alert to central IDS.

4.3. Signature based detection layer

Signature-based detection is middle layer that detects known threat. It compares the signatures with observed events to determine the possible attacks. Some known attacks are identified on the basis of implemented security policy. For example, if telnet tries to use "root' username that is violating the security policy of organization that is considered the known attack.

If operating system has 645 status code values that is indication of host's disabled auditing and refers as attack. If attachment is with file name "freepics.exe" that is alert of malware. Middle layer is effective for detection of known threats and using well-defined signature patterns of attack. The stored patterns are encoded in advance to match with network traffics to detect the attack. This layer compares log entry with list of signatures by deploying string comparison operation.

If signature based layer does not detect any network, anomaly based detection layer initiates the process. For example, if request is made for web page and to be received the message with status code of 403, it shows that request is declined and such types of processing cannot be tailored with signatures based layer.

4.4. Anomaly Based Detection Layer

Lower layer is anomaly based detection that identifies unknown and DOS attacks. It works on pick-detect method. This method monitors the inbound and outbound traffic received through central IDS. Packets are evaluated, adaptive threshold and mean values are set. It calculates the metrics and compares with threshold [26] & [27].

On the basis of comparisons, it detects various types of anomalies including false positive, false negative, true positive and true negative. If pick-detect methods determines true positive and false negative then it sends alert to Central IDS. The process of determining the anomalies is given in algorithm 2.

Algorithm 2: Detecting the types of alerts with AIDS

1. FA= Frame of signatures
2. FA $\subseteq$ AIDS
3. Si = False Negative
4. Sj= True negative
5. Sk= True positive
6. Sl= False positive
7. 0 = don't match & 1= match
   m
8. Sijkl = 1/d $\sum$ Sijkl
            m=1
9. Sij = { 0, if i & j
10. No false negative & true positive
11. Sij = { 1, if i & j
12. false negative & true positive
13. Alert of attack
14. Skl = { 0, if k & l [do not match] & 1, if k & l [match]
15. Alert of true negative & false positive
16. No sign of attack
17. endif
18. endif
19. endif
20. endif

In addition to determine and calculate true positive, true negative, false positive and false negative, the following derivation helps:

Here True positive= TP; False negative= FN; False positive=FP; True negative=TN; Precision= p; overall probability= OP

We know that

$P = TP/ TP + FP$ (1)
$OP= TP + TN / TP + FP + FN + TN$ (2)
$TP = P (TP +FN)$ (3)
Substitute the values of precision in equation no (2)
Therefore,
$TP= TP/ TP + FP (TP +FN)$ (4)
OR
$TP = (TP * TP) + (TP + FN) / TP + FP$ (5)
OR

$$TP= TP^{2 +} (TP* FN) / TP + FP$$

The equation (5) shows the true positive (TP), meaning that is sign of attack and alarm occurs
Now, find the false negative to apply overall probability formula:
We know that overall probability formula that is given as follows:
$OP= TP + TN / TP + FP + FN + TN$
$TP = OP (TP + FP + FN + TN) = TP + TN$ (6)
Substitute the value of OP in equation (6):
$TP = TP + TN / TP + FP + FN + TN (TP + FP + FN + TN) = TP + TN$ (7)
$(TP + TN) * TP + (TP + TN)* FP + (TP + TN) *FN + (TP + TN)*TN / TP + FP + FN + TN = TP +TN$ (8)
Multiplying the values:
$(TP^{2 +} TNTP) + (TP*FP + TN*FP) + (TP*FN + TN*FN) + (TP*TN + TN^2) = TP + TN (TP + FP + FN + TN)$ (9)
Re-arranging:
$(TP^{2 +} TNTP) + (TP*FP + TN*FP) + (TP*TN + TN^2)=(TP + TN (TP + FP + FN + TN) - (TP*FN + TN*FN)$
Multiplying the (TP + TN) to the right hand side:
$(TP^{2 +} TN*TP) + (TP*FP + TN*FP) + (TP*TN + TN^2) = (TP^2 + TN*TP +FP*TP +FP*TN+ FN*TP + FN*TN + TN*TP + TN^2 - (TP*FN + TN*FN)$ (10)
Simplifying the terms by using addition and subtraction function:
$FN*TN - FN*TN$ (11)
Finding the value of FN
$FN = FN * TN /TN$ (12)
Divide TN with FN *TN to get FN
$FN= FN$ (13)
OR

$$FN-FN= 0$$

If we get zero value that shows the false negative and considered as attack but no sign of alarm because of 0. The false positive (FP) is derived from true positive (TP). If we know that about the value of TP:
$TP= TP^2 + (TP * FN) / TP + FP$
Cross by multiplication to both sides:
$TP (TP + FP) = TP^{2 +} (TP + FN)$ (14)
Multiplying TP to the left hand side:
$TP^2 +TP*FP = TP^{2 +} (TP * FN)$ (15)
Re-arrange the terms:
$FNTP =TP^{2 +} TP * FP - TP^2$

FN*TP = TP * FP   (16)

Calculate the FP from equation (16):

FN*TP= FP/TP   (17)

OR

FP= FNTP /TP

The equation (17) shows the false positive; there is no sign of attack but alarm raised.
Applying equation (10) to find the true negative (TN).
Here,
FN*TN - FN*TN
FN*TN = FN*TN
TN = FN*TN/ FN   (18)
Dividing FN*TN by FN to find TN
TN= TN   (19)
OR

TN-TN=0

The value of TN is also zero that means there is no sign of alarm and no attack occurs.
To detect the attack and non-attack situation for TN and FN. We use algorithm 3 to determine sign of attack.

Algorithm 3: Determine the sing of attack or non-sign of attack

1. We select random odd prime number for TN and any even number for FN.
2. The value of FN must not be exceeded than TN.
3. Therefore, FN > 1 & FN< TN
4. Here, FN= {2, 4, 6, 8…} & TN= {3, 5, 7, 11, 13…}
5. Here sign of attack = ST, d = not exposed & b = exposed.
6. b and d has constant value 1.
7. Thus, ST = TN/ (TN+ d)/ FN (FN +b)
8. If value of ST > 1, it means there is no sign of attack, if the value of ST < 1 that is sign of attack.
9. endif
Assume FN = 2 & TN =3
BY applying the sign of attack formula:
ST = TN/ (TN+ d)/ FN (FN +b)
Substitute the values in given formula.
ST = 3/ (3+ 1) / 2(2+1)
ST = 9/8
ST= 1.125
ST > 1
ST > 1 means there is no sign of attack and we will be able to determine that is True negative (TN)

5. Simulation Setup

The previous sections have presented the evidence of the problems to be created by rogue DHCP server and including solution to control over these problems. This section focuses on simulation setup and analysis of the result. The unique and extensive testing method for rogue DHCP needs various kinds of intrusions to validate the claim. The basic purpose of testing is to

obtain the results in controlled and live user environments. However, overall target is to obtain the result in highly loaded network. We have used three types of simulation ns2, discrete simulation in C++ and testbed. We here discuss only testbed simulation. The testing procedure is done on two types of fast and slow systems. The slow system is used for capturing the attacks while fast is reserved for generating attacks. The simulation also uses Nikto that helps to detect the attacks from web applications because snort only captures the binary or data files. Snort stores these files in var /log/snort directory. They are analyzed with editor or simple network management protocol (SNMP) manager such as Open NMS [14] & [15]. MySQL database is used to create the alert data. Other database such as oracle can also be used but we give priority to MySQL because used Snort-2 IDS is more suitable and familiar with this. Apache web server is also part of this simulation that supports HTTP-based web server.

To create the interface between web server and MySQL, we use PHP that links both successfully. PHP package also uses Analysis Console for Intrusion Databases (ACID) that is supportive for analyzing the snort data. After analysis the packets, gif draw (GD) library is used to make graphs and these graphs are presented with help of (PHPLOT). ACID needs to be connected with MySQL to analyze the data. So, it uses Active Data Objects Data Base (ADODB). To monitor the performance of IDS, stress test utility (Stick) is used that generates the higher amount of malicious traffic and conceals the false attack in order to test the functionality of IDS. The detail of parameters used for simulation is given in table 1.

TABLE 1: Simulation parameters for experiment

Name of parameters	Specification	
MySQL database	MySQL 5.5	
Type of IDS	Rule based IDS	
GD Library	gd 2.0.28	
Snort	V-2	
Apache web server	Apache http 2.0.64 Released	
PHP	PHP 5.3.8 (General purpose server side language)	
Stick	Stick beats detection tool used by hackers	
Nikto	*Nikto* v.2.1.4	
IDS enabled system	Memory	512 MB
	Operating system	Linux
	PCI network card	10/100 Mbps
	CPU	P-III with 600 MHz
Attacker system	Operating System	Linux
	Memory	1.5 GB

PCI Network card	10/100/1000 Mbps
CPU	AMD Geode LX running 2.4/5GHz

6. Analysis of Result and Discussion

The training period of experiment covers four classes of attacks probe, DOS, U2R and R2L. The experiment sets the value of minimum frequency to 1 and relates the number to valid time. So, detected attacks are included in database during the training period. The MSAIDS scans all of the rules of snort and includes new rules explained in proposed section 3. The testing period targets several concise scenarios. The scenarios are simulated by using same parameters for all of the three existing schemes and one for our proposed MSAIDS scheme. The attacks are generated by using stick, covering all types of signatures and anomaly based attacks.

The training period provides quite interesting results because frequently generated attacks are of different numbers. The maximum number of attacks pertains to R2L category. The more attacks are also counted on MSAIDS as compare with other three existing techniques are shown in table.2. If attack is not generated then it is counted as normal traffic. The frequency of single and group characters is displayed when packets reach at the attacker machine and they are analyzed. It is observed on the basis of output that different types of detected attacks to be generated due to rogue DHCP server.

The DOS attacks are detected when packet does not reach at destination and received no acknowledgment. The sign of probe attack is addition of new data in existing amount of data bytes that shows the alteration in the original data. U2R is the sign of maximum connection duration. R2L attacks are more complex to detect because they use host and network based features. Therefore, we apply method comprises of service requested and duration of connection for network and attempts failed login for host.

It shows that proposed approach does not restrict the generating ratio of packet. From other side, the proposed work provides promising capturing ratio for signature as well as anomaly based attacks. The statistical results show that MSAIDS will substantiate to medical field for diagnosing several disease and especially for heart. The major breakthrough of this research is to detect the true positive and false negative attacks because they are very hard to capture.

TABLE 2: showing statistical data for attack

Type of generated attack	Multi frame signature-cum-anomaly based IDS (MSAIDS)	Dynamic Multi-Layer Signature based IDS (DMSIDS)	Ant Colony Optimization based IDS (ACOIDS)	Signature based IDS
DOS attacks	34214	33542	33421	32741
U2R attacks	12454	11874	11845	11341
R2L attacks	34123	32123	31092	29984
Probe attacks	6214	8758	10181	4907

Due to these anomalies, confidentiality of any system is exploited and privacy of the user is exposed. The proposed method also captures the real worm attacks and all other looming attacks. The proposed approach is highly supported with new rules, mathematical model and

algorithms that collectively make the MSAIDS smarter and quite successful. The table 3 shows quantitative results for each scheme.

TABLE 3: Showing quantitative data for proposed and existing schemes

Parameters	Multi frame signature-cum- anomaly based IDS (MSAIDS)	Dynamic Multi-Layer Signature based IDS (DMSIDS)	Ant Colony Optimization based IDS (ACOIDS)	Signature based IDS
total no: of packet to be received	236719	198678	201938	178109
total no: of packet to be analyzed	236456	192453	197842	170098
total no: of attack to be generated	87005	86293	86539	78973
total no: of signature based attack to be generated	42003	42287	42585	35098
total no: of anomaly based attack to be generated a. False positive b. False negative c. True positive d. True negative	a. 9475 b. 12093 c. 18574 d. 4860	a. 8574 b. 11987 c. 16943 d. 6502	a. 8878 b. 12007 c. 16943 d. 6126	a. 8458 b. 11289 c. 12455 d. 11673
Total number of anomaly based attack to be generated	45002	44006	43954	43875
total no: of attacks to be captured	87002	84212	83434	36098
Anomaly based attacked captured a. False positive b. False negative c. True positive d. True negative	a. 9475 b. 12093 c. 18574 d. 4859	a. 8324 b. 11456 c. 15678 d. 6324	a. 8678 b. 11987 c. 16789 d. 6045	a. 654 b. 245 c. 453 d. 535
total number of anomaly based attacks to be captured	45001	41782	43499	1887
signature based attacks to be captured	42001	42102	41091	34211

The major advantage of MSAIDS approach is to detect all types of anomalies and unknown threats efficiently. The systems are mostly infected due to new sort of malwares because they consume the processing resources of system. If resources of system are utilized by unnecessary programs then MCL is highly affected. In consequence, collaboration process is disrupted. MSAIDS also detects the activity for any specific session. It creates specific alarm for each type of anomalies. The figures 7 to 10 show the capturing capability of anomalies and compares with other well known techniques. The implementation of MSAIDS is also

supported with sound architectural design. Statistical data is highly encouraging that shows 99.996% the overall capturing capability of all types of signatures and anomaly based attacks.

The overall capturing capability of MSAIDS is calculated with following formula.
Here, overall Capturing capability = E_a; total generated signature based attacks = TSA;
Total anomaly based attacks =TAS; missed signature based attacks = MSA;
Missed anomaly based attacks = MAA & total generated attacks = TGA.
Thus, E_a = (TSA + TAA) – MSA + MAA) * 100 / TGA

On basis of given formula, we prove overall strength of MSAIDS technique that is given in figure 11.
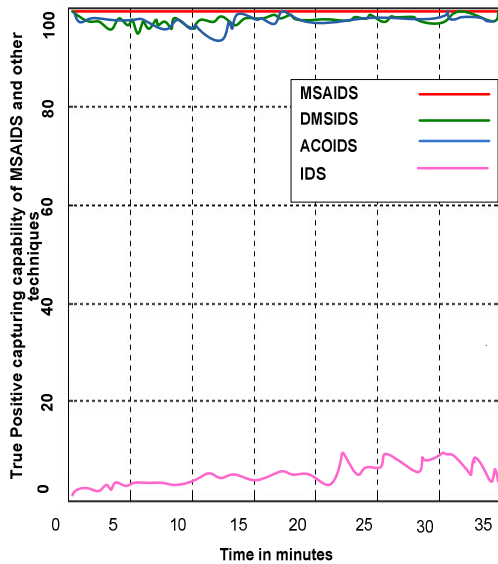

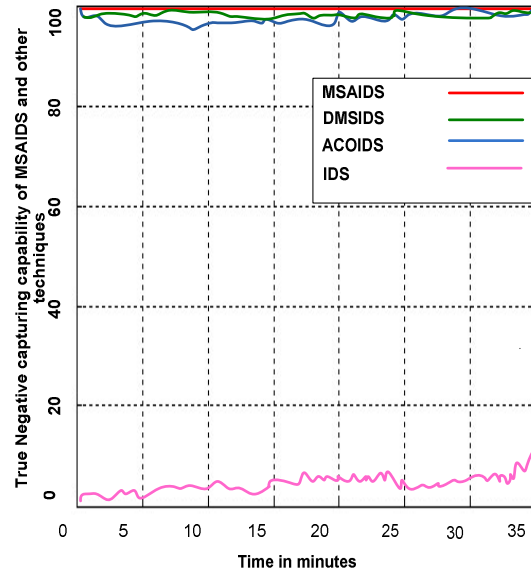Fig. 7. True positive anomaly % at different time interval Fig.   8. True Negative anomaly% at different time interval
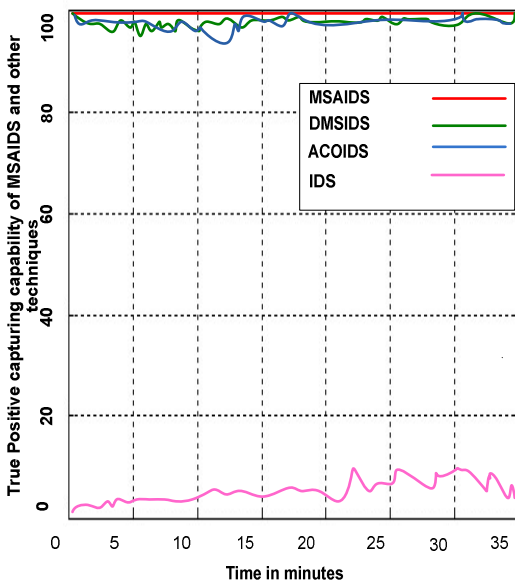

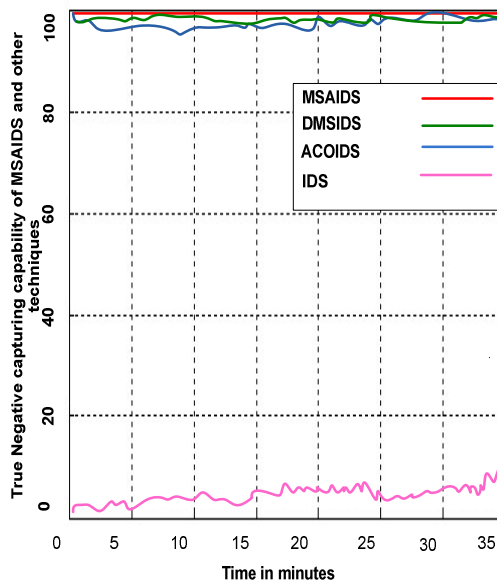Fig..9. True Positive anomaly% at different time interval   Fig. 8. True Negative anomaly% at different time interval
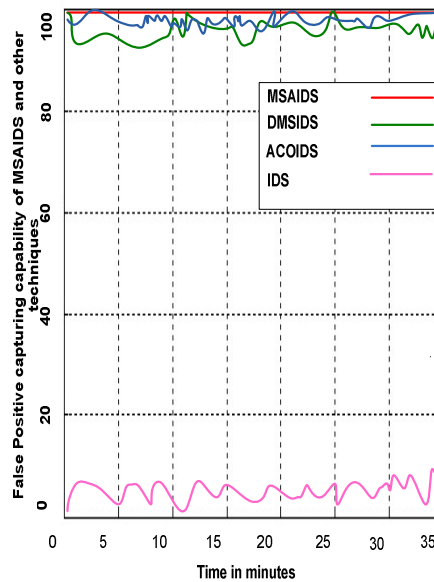
Fig. 10. False positive anomaly% at different time interval

7. Conclusion

In this paper, multi-frame signature-cum anomaly-based intrusion detection systems (MSAIDS) is proposed. MSAIDS controls malicious activities of DHCP rogue server to restore the privacy of users during MCL. The paper highlights all the malicious threats to be generated by DHCP rogue. The intruders use the DHCP server to sniff the traffic and finally deteriorate the confidential information. The mechanism of current IDS does not have enough capability to control the threats. Furthermore, several daunting and thrilling challenges in the arena of computer network security are impediment for secure communication. DHCP rogue is visibly very simple but crashes the network as well as the privacy of the users and even creates nastier attacks like Sniffing network traffic, masquerading attack, shutting down the systems and DOS. The first is detailed explanation of these attacks and how they are generated by DHCP rogue. To resolve this issue, second propose the technique that is based on algorithms, mathematical modeling and addition of new rules in current IDS. These all of the components of proposal collectively handles the issues of DHCP rogue. To validate the proposal, the technique is simulated by using two different kinds of systems, as one is reserved for attacker and other one is for legitimate user.

On the basis of simulation, we obtain very interesting statistical data, which show that MSAIDS improves the capturing performance and controls the attacks to be generated by DHCP rogue as compare with original IDS and other techniques. The findings demonstrate that MSAIDS has significantly reduced the false alarms.

Finally, we analyze the overall efficiency of MSAIDS and existing technique by showing the results in tabular form and plotting the impact of results. In future, this technique will be deployed to measure the heart beats and other disease. Furthermore the broader impact of this research is to substantiate the MCL and improve the pedagogical activities and fostering other organizational requirements. This research will also boost the confidential level of the people while using MCL.

References

[1] AdityaVidyarthi and A. S. Saxena, "Conceiving a intrusion detection system in the network by mobile agents" ,International Journal of Computer Science and Communication Vol. 2, No. 2, July-December 2011, pp. 497-499

[2] MueenUddin, Kamran Khowaja, Azizah Abdul Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[3] S. Janakiraman, V. Vasudevan, "ACO based Distributed Intrusion Detection System", International Journal of Digital Content Technology and its Applications Volume 3, Number 1, March 2009.

[4] D. Boughaci, H. Drias, A. Dendib, Y. Bouznit, and B. Benhauou, "Distributed intrusion detection framework based on autonomous and mobile agents", Proceedings of the International Conference on Dependability of Computer Systems, pp. 248-255, May, 2006.

[5] MikroTik, "DHCP Client and Server", document revision 2.7, V2.9, 2005.

[6] Dayong Ye, QuanBai, and Minjie Zhang, "P2P Distributed Intrusion Detections by using Mobile Agents", Seventh IEEE/ACIS International Conference on Computer and Information Science, IEEE Computer Society, pp. 259-265, IEEE, 2008.

[7] Microsoft Windows DHCP Team Blog,"Rogue DHCP Server"from website: detectionhttp://blogs.technet.com /03/rogue-dhcp-server-detection.aspx.

[8] Overview of DHCP Snooping, "Catalyst 6500 Series Switch Cisco IOS Software Configuration Guide, Release 12.2SX", 2010.

[9] . Sherri Davidoff, "How to defend against rogue DHCP server malware", published first time on 2009. From website: www.searchsecurity.techtarget.com.

[10] DalilaBoughau, HabibaDrias, Ahmed Bendib, YoucefBouznit and BelaidBenhamou, "A Distributed Intrusion Detection Framework based on Autonomous and Mobile Agents", Proceedings of the International Conference on Dependability of Computer Systems (DEPCOS RELCOMEX'06), IEEE Computer Society, IEEE 2006.

[11] William stallings' " Network security essentials: Applications and standards, Fourth Edition.

[12] Hitesh Ballani, Paul Francis, "Mitigating DNS DoS Attacks", ACM, CCS'08, Alexandria, Virginia, USA, October 27-31, 2008.

[13] "UltrDNSDDoS Attack, Washington Post," May 2005, http://blog.washingtonpost.com/securityfix/2006/05/ blue security surrenders but s.html.

[14] .Rafeeq Ur Rehman,"Intrusion Detection Systems with Snort Advanced IDS Techniques Using Snort, Apache, MySQL, PHP, and ACID", Prentice Hall PTR Upper Saddle River, New Jersey 07458.

[15] MueenUddin, Kamran Khowaja, Azizah Abdul Rehman, "Dynamic Multi-Layer Signature Based Intrusion Detection System Using Mobile Agents", International Journal of Network Security & Its Applications (IJNSA), Vol.2, No.4, October 2010.

[16] "Akamai DDoS Attack, Internet Security News," Jun 2004, http://www.landfield.com/isn/mail-archive/2004/ Jun/0088.html.

[17] SaidatAdebukolaOnashoga, Adebayo D. Akinde,, Adesina Simon Sodiya,"A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems", Issues in Informing Science and Information Technology Volume 6, 2009.

[18] AdityaVidyarthi and A. S. Saxena, " Conceiving a intrusion detection system in the network by mobile agents" International Journal of Computer Science and Communication Vol. 2, No. 2, July-December 2011, pp. 497-499.

[19] Dewan Md. Farid, NouriaHarbi, Mohammad ZahidurRahman, " Combining naïve bayes and decision tree for daptive intrusion detection" International Journal of Network Security & Its Applications (IJNSA), Volume 2, Number 2, April 2010, PP. 12-25.

[20] K. Park and H. Lee. On the effectiveness of probabilistic packet marking for IP trace back under Denial of Service attack. In *Proc. IEEE INFOCOM*, Anchorage, AK, Apr. 2001.

[21] Sapna S. Kaushik, Dr. Prof.P.R.Deshmukh, "Detection of Attacks in an Intrusion Detection System", International Journal of Computer science and information technologies (IJCSIT) ISSN: 0975-9646, Vol. 2 (3), 2011.

[22] L. Garber. Denial of Service attacks rips the Internet. *IEEE Computer,* 33, 4:12–17, Apr. 2000.

[23] B. Abdullah*, Abd-alghafar, Gouda I. Salama, A. Abd-alhafez, "performance evaluation of a genetic algorithm based approach to network intrusion detection system", 13th International Conference on Aerospace Scientific and aviation technology (ASAT- 13, May 26 – 28, 2009.

[24] D. Moore, G. M. Voelker, and S. Savage. Inferring Internet denial-of-service activity. In *Proc. USENIX Security Symposium*, Washington D.C, Aug. 2001.

[25] Yan Yang and Mohamed S. Kamel, "An aggregated clustering approach using multi-ant colonies algorithms", The Journal of the Pattern Recognition Society, Elsevier, Vol. 39, pp. 1278-1289, 2006.

[26] G. Helmer, J.S.K. Wong, V. Honavar, and L. Miller, "Automated discovery of concise predictive rules for intrusion detection," Journal of Systems and Software, vol. 60, no. 3, 2002, pp. 165- 175.

[27] R.C. Chen, and S.P. Chen, "Intrusion detection using a hybrid support vector machine based on entropy and TF-IDF," International Journal of Innovative Computing, Information, and Control (IJICIC), vol. 4, no. 2, 2008, pp. 413-424.

[28] Anderson, J.P. (April, 1980). Computer Security Threat Monitoring and Surveillance. Technical Report,J.P. Anderson Company, Fort Washington, Pennsylvani.

BIOGRAPHY

Mr. Abdul Razaque is PhD student of computer science and Engineering department in University of Bridgeport. His current research interests include the design and development of learning environment to support the learning about heterogamous domain, collaborative discovery learning and the development of mobile applications to support mobile collaborative learning (MCL), congestion mechanism of transmission of control protocol including various existing variants, delivery of multimedia applications. He has published over 45 research contributions in refereed conferences, international journals and books. He has also presented his work more than 20 countries. During the last two years.

He has been working as a program committee member in IEEE, IET, ICCAIE, ICOS, ISIEA and Mosharka International conference. Abdul Razaque is member of the IEEE, ACM and Springer Abdul Razaque served as Assistant Professor at federal Directorate of Education, Islamabad. He completed his Bachelor and Master degree in computer science from university of Sindh in 2002. He obtained another Master degree with specialization of multimedia and communication (MC) from Mohammed Ali Jinnah University, Pakistan in 2008. Abdul Razaque has been directly involved in design and development of mobile applications to support learning environments to meet pedagogical needs of schools, colleges, universities and various organizations.

Dr. Khaled Elleithy: is the Associate Dean for Graduate Studies in the School of Engineering at the University of Bridgeport. His research interests are in the areas of, network security, mobile wireless communications formal approaches for design and verification and Mobile collaborative learning. He has published more than two hundreds research papers in international journals and conferences in his areas of expertise.

Dr. Elleithy is the co-chair of International Joint Conferences on Computer, Information, and Systems Sciences, and Engineering (CISSE).CISSE is the first Engineering/ Computing and Systems Research E-Conference in the world to be completely conducted online in real-time via the internet and was successfully running for four years. Dr. Elleithy is the editor or co-editor of 10 books published by Springer for advances on Innovations and Advanced Techniques in Systems, Computing Sciences and Software.

Dr. Elleithy received the B.Sc. degree in computer science and automatic control from Alexandria University in 1983, the MS Degree in computer networks from the same university in 1986, and the MS and Ph.D. degrees in computer science from The Center for Advanced Computer Studies in the University of Louisiana at Lafayette in 1988 and 1990, respectively. He received the award of "Distinguished Professor of the Year", University of Bridgeport, during the academic year 2006-2007