# Implementation of Hybrid Artificial Intelligence Technique to Detect Covert Channels Attack in New Generation Internet Protocol IPv6

Abdulrahman Salih[1], Xiaoqi Ma[2], and Evtim Peytchev[3]

## ABSTRACT

*Intrusion detection systems offer monolithic way to detect attacks through monitoring, searching for abnormal characteristics and malicious behavior in network communications. Cyber-attack is performed through using covert channel which currently, is one of the most sophisticated challenges facing network security systems. Covert channel is used to ex / infiltrate classified information from legitimate targets, consequently, this manipulation violates network security policy and privacy. The New Generation Internet Protocol version 6 (IPv6) has certain security vulnerabilities and need to be addressed using further advanced techniques. Fuzzy rule is implemented to classify different network attacks as an advanced machine learning technique, meanwhile, Genetic algorithm is considered as an optimization technique to obtain the ideal fuzzy rule. This paper suggests a novel hybrid covert channel detection system implementing two Artificial Intelligence (AI) techniques; Fuzzy Logic and Genetic Algorithm (FLGA) to gain sufficient and optimal detection rule against covert channel. Our approach counters sophisticated network unknown attacks through an advanced analysis of deep packet inspection. Results of our suggested system offer high detection rate of 97.7% and a better performance in comparison to previous tested techniques.*

**Keywords**: Cyber-attack; Covert channel; ICMPv6; IPv6; Fuzzy Genetic Algorithm (FGA); AI;

## 1. INTRODUCTION

The growth of dependability on the Internet in every day services made people susceptible to all kinds of cyber-attacks such as; fraud, spam, phishing and all types of unauthorized access through ID theft. Despite the fact that the security issues in IPv6 were addressed and improved, other issues are still need to be investigated due to the inherited design vulnerability and the incomplete implementation process of this protocol in all operating systems (Zander et al. 2006). The protocol itself is already over a decade old, however its approvals early stages reaching 10 % according to latest statistics performed (Salih et al. 2015)

[1] Abdulrahman Salih is a PhD candidate at Nottingham Trent University. He received his MSc with Distinction in IT Security from University of Westminster, London in 2010, and his BSc (Horns) Software Engineering from Nottingham Trent University in 2007. He worked as a Network Security Engineer for Planet Solutions in London before rejoining NTU. He is the founder and CEO of KNCIS in Sweden-UK, specializing in Cyber Security Analysis. FB104480@ntu.ac.uk

[2] Dr Xiaoqi Ma is a Senior lecturer and a leader of many modules; Security Technologies, Computer Security and Advanced Security Technologies in the School of Science and Technology at Nottingham Trent University. He is a member of the Intelligent Simulation, Modelling and Networking Research Group (ISMN). He obtained PhD from Reading University in 2007 in Cryptographic Network Protocols. He contributed in more than 20 publications in International Journals, conferences and book chapters, xiaoqi.ma@ntu.ac.uk

[3] Dr Evtim Peytchev is a Reader in Wireless, Mobile and Pervasive Computing in the school of Science and Technology at Nottingham Trent University, UK. He is leading the Intelligent Simulation, Modelling and Networking Research Group, which consists of 5 lecturers, 3 Research Fellows and 6 research students. He is the Module Leader for Systems Software; and Wireless and Mobile Communications. He also teaches on the modules Software Design and Implementation; Mobile Networking; Enterprise Computing; and Computer Architecture, evtim.peytchev@ntu.ac.uk

The low and inevitable acceptance of IPv6 results in an insufficient understanding of its security properties (Martin & Dunn, 2007), (Supriyanto et al. 2012) IPv6 had no cryptographic protection when deployed and even the successful deployment of Internet Protocol Security (IPsec) within IPv6 cannot give any guarantee or additional security against hidden channel attacks (Zander et al. 2006), (Supriyanto et al. 2012).

The protocol dimension representing the removed, changed and new values in the header fields according to its suggested new design by the Interned Assigned Numbers Authority (IANA) and Request For Comments (RFC 2460) (Martin & Dunn, 2007), (Zander et al. 2006). IPv6 header fields as shown in Table 1 have potential to carry anomaly attacks depending on the modified value of each field in the packet transmission over the net (Supriyanto et al. 2012) (Choudhary, 2009), (Wendzel et al ., 2015).

There are two main types of Intrusion Detection System (IDS) techniques can perform security analysis; the anomaly detection method and the misuse detection (signature based) method. Anomaly detection depends on the conventional profile in order to identify any abnormality in the traffic, whereas signature based detection uses signature identification technique to detect attacks (Gomez & Dasgupta, 2002), (Liu & La, 2009). Interestingly, three important techniques are used by misused detection approach:

1. Signature-based approaches
2. Rule-based approaches or also called expert systems.
3. Genetic Algorithms (GA)

Internet Control Message Protocol version 6 (ICMPv6) is a vital component and an integral part of IPv6 and should be fully implemented by every IPv6 node according to RFC (4443), however this particular aspect obviously means hidden channels (Martin & Dunn, 2007). ICMPv6 reports errors encountered in processing packets (Choudhary, 2009) and it does other Internet-layer functions such as; diagnostics. It produces two types of messages: Information Notification and Error Notification. It uses Type and Code fields to differentiate services, in which both are vulnerable to be misused by bad guys to perform different attacks i.e. denial of Service (DoS), Man-in-the-Middle (MITM) and spoofing attacks (Martin & Dunn, 2007), (Supriyanto et al. 2012), (Choudhary, 2009).

**Table 1.** Extracted IPv6 Header Fields and Their Format Values

| ID | Field | Covert Channel | Bandwidth |
|---|---|---|---|
| 1 | Traffic Class | Set a false traffic class | 8bits/packet |
| 2 | Flow Label | Set a false flow label | 20 bits/packet |
| 3 | Payload Length | Increase value to insert extra data | Various |
| 4 | Next Header | Set a valid value to add an extra extension header | Various |
| 5 | Hop limit | Increase/decrease value | ≈ 1 bit/packet |
| 6 | Source Address | Set a false source address | 16 bytes/packet |

In this paper, we suggest a new hybrid approach using fuzzy logic and genetic algorithm to detect network storage covert channels in IPv6. The process analyses the IPv6 and ICMPv6 header fields values and explains the viability of holding strange values which consequently indicating an abnormal behavior and possible covert channel existence.

The rest of the paper is organized as follow: Section 2 describes briefly some related works, Section 3 discusses the proposed research methodology, the theory and techniques

implemented, Section 4 discusses the experiments and initial results obtained from the testing phases, and finally Section 5 discusses Conclusions and Future work.
Our proposed security system offers a better performance in high accuracy and prediction of the future unknown attacks against legitimate targets.

## 2. RELATED WORK

Previous researchers in network anomaly detection focused on IPv4 (Zander et al. 2007)), (Sohn et al. 2003), (Vivek & Kalimuthu, 2014), however fewer researchers were concerned about security vulnerabilities of the new generation protocol IPv6 due to its incomplete implementation. Hidden information could be transferred very easy in the data section of the packet due to the large size and it's relatively unstructured in comparison to headers.

Salih et al. (2015) argue that covert channels could be encoded in the unused or reserved bits in the packet header frame, these unused header fields are designed for future protocol improvements, as they will be dismissed by IDS and Firewalls (Zander et al. 2007), (Supriyanto et al. 2012), (Liu & Lai, 2009) furthermore this exception caused by the presence of specific values in protocol standards (Martin & Dunn, 2007), (Zander et al. 2006). Different machine learning techniques have been used in IDS in a revolutionary status since 1990's. Genetic algorithm started to be used in IDS since 1995 when Crosbie and Spafford (Jongsuebsuk et al. 20013), applied a hybrid approach of a multiple agent and Genetic Programming (GP) to detect network anomalies. GA is used in many proposed approaches in intrusion detection techniques due to its intensive capabilities.

Sohn et al. (2003) mentioned the Support Vector Machine in passive warden to detect TCP anomaly within the IP ID and TCP ISN. This method was not preferable for well understood and explicit features in his proposed IP IDs and ISNs steganography hidden communication channels, furthermore SVM can only identify simple aspects as it could unlikely detect complex structure deployed in TCP/IPv6 fields and their inter-dependencies.

Gomez and Dasgupta (2002) suggested fuzzy and genetic algorithm to detect and classify behavioral intrusion suing a bench mark data KDD99 dataset. They used evolutionary techniques and genetic algorithm which managed to classify 4 attack classes and one normal class.

Salih et al. (2015) proposed new Intelligent Heuristic Algorithm (IHA) with an enhanced machine learning technique; Nave Bayes classifier to detect covert channels in IPv6. The authors used enhanced decision trees C4.5 and Information Gain to improve the detection rate. Accuracy in this approach was 94% with very low false negative rate.

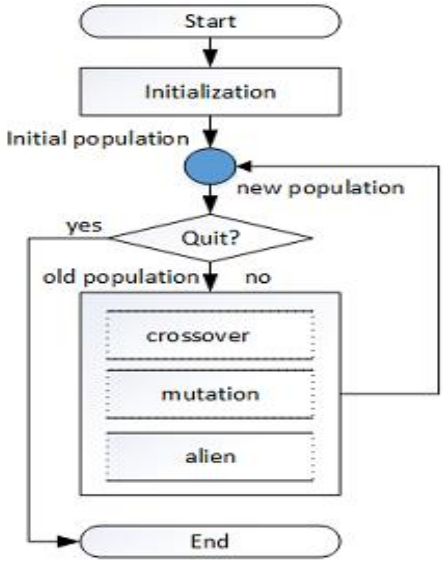
## 3. PROPOSED FRAMEWORK

Different approaches exist for anomaly detection i.e. signature, behavior and protocol based detection. Infrequent researchers use machine learning technique to tackle anomaly attacks in IPv6 and ICMPv6 due to its incomplete implementation and design complexity (Zander et al. 2007). Our approach uses pattern behavior of the header value to determine the identified data that has been transferred stealthily by the attacker using covert channels without affecting the normal communication.

### 3.1 Fuzzy Genetic Algorithm (FGA)

Genetic Algorithm is an evolutionary Artificial Intelligence (AI) optimization technique based on some synthetic keys such as natural selection and genetics (Chen et al. 2008). Fries (2008) verified that John Holland with his academic colleagues at the University of Michigan have invented GA in the 1960s and the 1970s, explained the mechanism behind it. GA is based on Darwinians biological principle of evolution: The survival of the fittest. It uses three dominant functions; selection, crossover and mutation when optimizing a population of candidate solution and to predefine fitness. This algorithm has been successfully implemented (Jongsuebsuk et al. 20013), (Hoque et al. 2012) to solve significant collection of complex optimization problems when search area is too broad. We propose an enhanced version of (Fries, 2008) rule-based algorithm with new and different attacks i.e. covert channels in the new generation network protocols IPv6/ICMPv6. The framework uses new simulated primary data and NSL-KDD99 benchmark data to verify the results. The suggested Fuzzy Genetic Algorithm (FGA) as shown in Figure 1 can perform classification process of two classes; normal and anomaly with an improved high detection rate.

**Fig 1.** Suggested Genetic Algorithm Process to Tackle Covert Channel Attacks




The following steps are the main modules in the framework. An overview of the algorithms example is given in Algorithm 1, Algorithm 2 and Algorithm 3.

1. Data Capture: Jpcap library packet sniffer is a Java API used to capture simulated packets for 2 minutes and dissection process is done to extract the targeted IPv6 and ICMPv6 header fields as shown in Table 2.

**Table 2.** Covert Channels Data Format and Values

| *ID* | *Header Format* | *Value Type* | *Class* |
|---|---|---|---|
| *1* | Traffic_Class | Numeric | Normal or Covert |
| *2* | Flow_Label | Numeric | Normal or Covert |
| *3* | Hop_Limit | High,Low, Moderate | Normal or Covert |
| *4* | Payload_Length | increased,decreased, Low | Normal or Covert |
| *5* | Source_Address | Numeric | Normal or Covert |
| *6* | Next_Header | Numeric | Normal or Covert |
| *7* | ICMPv6_Type | Numeric | Normal or Covert |
| *8* | ICMPv6_Code | Numeric | Normal or Covert |
| *9* | Reserve_Bit | Numeric | Normal or Covert |
| *10* | ICMPv6_Payload | Numeric | Normal or Covert |

2. Packet Analysis: In this stage the input pcap data after field selection process will go through the following sub processes:
    a. Transform and normalize every attribute of the header to some sort of a real number giving the range of 0.0 7.0, in which means the minimum and the maximum subset values of the attribute from the training data will set in a range of 0.0 and 7.0.
    b. After transformation and normalization processes to the attributes and convert them to numerical formats, detection rules will be suggested as shown in Table 3 and Table 4 for all records. The output of the detection rule will be the probability of each packet and will count for true positive and true negative. The algorithm randomly will create a rule in the initial stage. Then an evolutionary concept is used from GA to improve the rule in the training state.
    c. We need to extract the records according to the rules, processing the fitness function in equation 1 to calculate the fitness value of each detection rule. Occasionally save the highest fitness value which indicates the best rule.

3. Process the evolutionary GA approaches; crossover, mutation and alien to extract the next rules.

### 3.2 Fuzzy Algorithm (FA)

In this stage, we encode a fuzzy logic for each attribute, then normalize the subset value in a range of 0.0 to 7.0 as mentioned above. The encoded fuzzy logic rule is explained in Algorithm 1. So every single rule will involve 10 blocks of feature values as shown in Table 2 including the class type at the end of the string, then each rule will be mapped to its correspond record as shown in Figure 2.

Once we run the rule over a record trying to match each attribute with one block of the rule. The probability measurement whether is an attack or not will be performed by the parameter of each block using the Fuzzy rules as shown in Algorithm 1. An assessment of the probability for each block will be done to predict the likelihood if the record is an attack class or a normal class, this is done through taking into account the average of the probability against the threshold mean value.

**Table 3.** Fuzzy Logic Detailed For Each Data Record

| **Data Type** | **Value** | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Fuzzy Logic | 0 | 1 | 0 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 0 | 1 |
| Symbol | a | | | b | | | c | | | d | | |
| Numeric | 2 | | | 3 | | | 4 | | | 5 | | |

Then we compare the predicted output against the actual result as in (Fries, 2008), furthermore, we will calculate the rule measurement performance through maximization of the fitness function using the equation (1) below as its embedded in Algorithm 2.

$$fitness\ function = \frac{a}{A} - \frac{\beta}{B} \qquad (1)$$

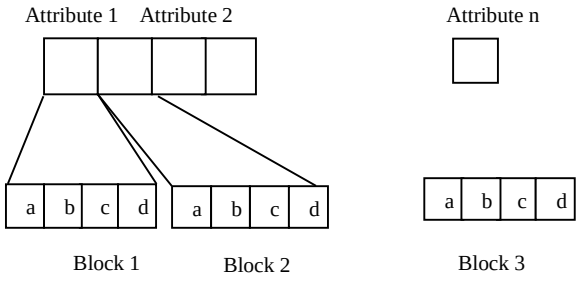



**Fig 2.** Explained String Encoding

### 3.3 Genetic Algorithm

Principally, not all attacks against legitimate targets have static patterns, however fuzzy logic will detect both types; normal and abnormal. The suggested fuzzy logic as shown in Table 3 is encoded into four parameters; a, b, c, and d where

$$a \leq b \leq c \leq d$$

According to a trapezoidal shape (Fries, 2008) it is very likely to be capable using the parameters to measure the likelihood of the attack through each attribute as described shown in Algorithm 3.

**Algorithm 1.** Fuzzy logic based on (Jongsuebsuk et al. 20013) with some modifications and corrections

```
If (value >a) && (value <b) {
        specificity = (value – a) / (b-a)
}
else if ( value ≥ b and value ≤ c) {
        specificity = 1.0;
}
else if (value > c and value < d) {
        specificity = (d – value) / (d-c)
}
else {
        specificity =0.0
}
```

### 3.4 Pre-processing Simulation Data

We performed two experiment tests on our suggested model; first, we used our simulated attack tool built and written in Python programming language (Scapy) to simulate attacks in a controlled LAN network lab environment. A sample of the covert channel's attack is shown in Table 5, then we captured packets in pcap format using Wireshark. The attribute instances from the header values have preprocessed into transformation, discretization (Wendzel, 2015), and normalization as mentioned in packet analysis section. According to previous research performed by Salih et al (2015) a new limited generation of covert channels primary data will be created including instances of different possible attacks in IPv6 and

ICMPv6. The primary data consists of 600.000 records in which contain more than 10 attack instances. The objective tested attacks are; Covert channels, Denial of Service (DoS), Probing and R2L.

### 3.5 Evaluation Criteria Parameters

To evaluate the performance of the algorithm, we used the following three metrics:

- False positive rate (FPR): ratio of normal packets will be classified as attacks out of the total normal packets accounts.
- False negative rate (FNR): ratio of attacks that misclassified as normal from total numbers, but it is attack.
- True Positive & True Negative (Detection rate): is the total normal and attacks that have been correctly classified out of the whole testing data.

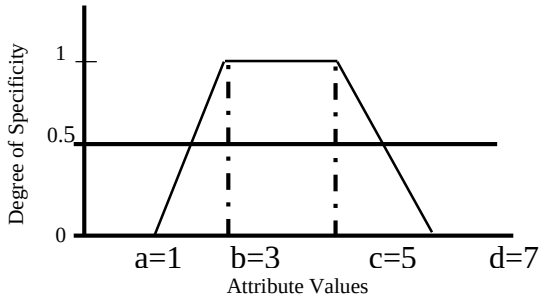
**Table 4.** Suggested Fuzzy Logic Encoding For Each Attribute

| 010 | 011 | 100 | 101 | 010 | 011 | 101 | 111 | 010 | 011 | 100 | 101 | 101 | 011 | 100 | 101 | covert |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| a=2 | b=3 | c=4 | d=5 | a=2 | b=3 | c=5 | d=7 | a=2 | b=3 | c=4 | d=5 | a | b | c | d | |
| Attribute 1 | | | | Attribute 2 | | | | Attribute 3 | | | | Attribute 10 | | | | class |

**Algorithm 2.** Fuzzy Genetic Algorithm is based on algorithm in (Fries, 2008) with few corrections.

```
Initial rules ();
while {
    For each packet {
        for each rule {
            for each attribute {
                specificity = fuzzy ();   // Algorithm 1
                total= total +specificity;
        }
            If (totalprob > threshold)
            class is attack;
            else
            class is normal;
            }
 compare the predicted result with actual result
find A, B, α, and β,
                    }
calculate fitness       // create next generation
preserve_best ()
crossover ()
mutation ()
alien ()
}
// A is total number of attack records. B is total number of normal records. α is total number
of attack records correctly identified as attack  β is total number of normal records
incorrectly classified as attack (false positive).
```

**Fig 3.** A Fuzzy Logic Trapezoidal Represented Four Parameters; $A \leq B \leq C \leq D$.




## 4. EXPERIMENT AND RESULT DISCUSSION

In the first step of the proposed framework, we designed and configured a separate IPv6 LAN topology network as shown in Figure 4 according to the network system environment requirements. A Security tool was created along with THC in (Hauser, 2015) to simulate different attacks in both protocols; IPv6 and ICMPv6 (Martin & Dunn, 2007), (Supriyanto et al. 2012).

We implemented the system using Weka 3.7 database system built with java programming Language and performed on personal computer with 3.1 GHz Inter core i5 CPU 3450 and 8 GB RAM. With regards to the GA implementation, we focused on 10 sizes of the population for each generation, however each individual will present a possible detection rule, and we chose two best individuals or rules, in which should have the highest fitness value from the present generation. We used uniform random as a selection method to select the parent in crossover process, this is to identify the members of the new generation, finally applying the single-point crossover in which will give the implemented rate of 20% for alien and 30% for mutation.

**Table 5**: Sample of Simulated Attacks Using Covert Channels in IPv6

| Attack Test Case | Performed Commands |
|---|---|
| Payload fields covert channels | `-send(IPv6(dst= "2001:db6:675c:7000::1") /IPv6DestOpt(options= [PadN(optdata=("22222222") )]+[PadN(optdata= ("3333333333333333"))]) / ICMPv6EchoRequest(id=1))` |
| Covert channel Using PadN Option | `-IPv6DestOpt(type=02data= ”YYYYY”)/icmpechorequest` |

The training dataset contained 11 attributes or features including the one target value or labelled class either normal or attack (covert) as shown in Table 6. We performed two experiments; first test was for the known attacks simulated from rules using Fuzzy Genetic Algorithm depicting two main attacks DoS and Probe using the primary dataset as a test data. In the second test, we evaluated our approach on a bench mark data such as Network Simulation Language Knowledge Data Discovery (NSL-KDD’99) choosing 20 % of the dataset for testing phase in order to detect known and unknown attacks (Tavallaee et al. 2009).

**Algorithm 3** The Fuzzy logic to identify 3 known attacks.

```
{
If (dos_rule =1 || probe_rule=1 || R2L=1)
        It is attack;
else if
If (dos_rule = 0 || probe_rule= 0 || R2L= 0)

        it is normal;
        end if
        }
```

- **Experiment 1**: The size of the primary dataset was not suitable to be used as testing data, so we chose 10 % for a training dataset in the first attempt consisted of 60,000 instances, although the process focused on detecting the following attacks instances:
    - Probe
    - Denial of Service (DoS)
    - Root to Local (R2L).

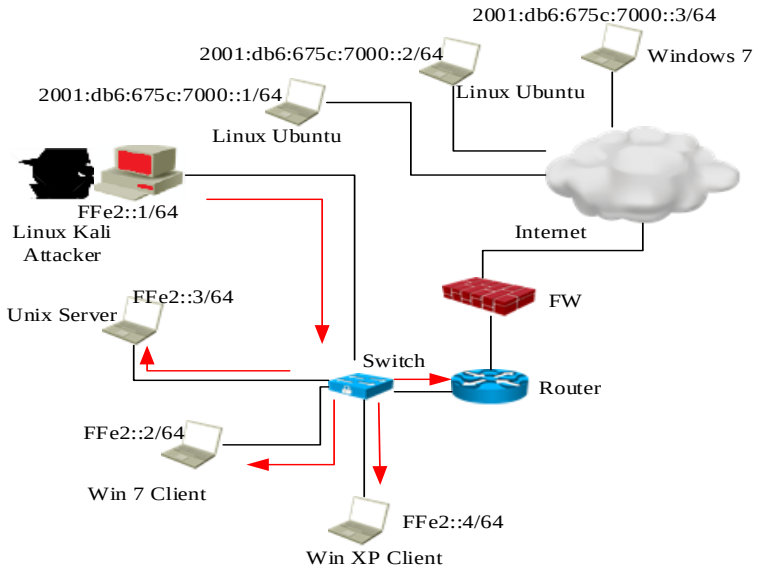



**Fig 4.** Configured IPv6 LAN Network Topology to Perform Attack Simulation

The first experiment results shown in Table 7 and the graph in Figure 4, we observe significant accuracy rates of the suggested approach detecting; DoS training dataset by 95.3%, the Probe attack detection by 96.8%, and R2L accuracy detection by 97.7% with a false positive rate by 3.7%. However when we performed the testing phase overall of the attack types the results have increased to 97.7% and the false positive decreased to 1.7% which shows a better performance and high accuracy improved by using the suggested FG Algorithm.

**Table 6**: Analysis Output Format of Covert Channel Characteristics

| R # | TC | FL | HL | PL | NH | SA | Type | Code | RB | PYL | Class |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | 0 | 0 | High | Increased | 0 | 0 | 0 | 1 | 0 | 1 | Covert |
| 2 | 1 | 1 | Low | Unchanged | 1 | 1 | 1 | 0 | 1 | 1 | Covert |
| 3 | 1 | 1 | Moderate | Descreased | 1 | 1 | 0 | 0 | 0 | 0 | Normal |
| 4 | 1 | 1 | Moderate | Decreased | 1 | 1 | 0 | 1 | 0 | 0 | Normal |
| 5 | 1 | 1 | Low | Unchanged | 1 | 1 | 1 | 0 | 1 | 1 | Covert |
| 6 | 1 | 1 | Moderate | Decreased | 1 | 1 | 0 | 0 | 0 | 0 | Normal |
| 7 | 0 | 1 | Moderate | Unchanged | 1 | 1 | 1 | 0 | 1 | 1 | Covert |
| 8 | 1 | 1 | Low | Unchanged | 1 | 1 | 0 | 0 | 1 | 1 | Covert |
| 9 | 0 | 1 | Moderate | Unchanged | 1 | 1 | 1 | 1 | 0 | 0 | Covert |
| 10 | 1 | 1 | Low | Unchanged | 1 | 1 | 1 | 0 | 1 | 1 | Covert |

- **Experiment 2**: In order to extend the proficiency of the proposed model and to validate it, we used the NSL-KDD99 dataset (Tavallaee et al. 2009). This dataset was collected at the Massachusetts Institute of Technology (MIT) in Lincoln Lab to evaluate intrusion detection systems, however it lacks instances of IPv6 attack types except the ICMPv4, and IP ID covert channels (Zander et al. 2007) which have similar principle techniques manipulating such attacks. McHugh and Mahoney in (Mahoney & Chan, 2003) criticized the DARPA dataset for not containing some background noise i.e. packet storms, strange packets, etc.

**Table 7.** Results of Primary Data Using FGA to Detect Different Attacks.

| Attack Name | Attack Type | Total Packets | Test Data | TPR % | FPR % | DR % |
|---|---|---|---|---|---|---|
| Smurf | DoS | 27,500 | 10.000 | 94.8 | 5.2 | **95.3** |
| Pod | DoS | | | 95.8 | 4.2 | |
| Teardrop | DoS | | | 97,8 | 2.2 | |
| Covert Channels | DoS | | | 94,6 | 5.4 | |
| Ipsweep | Prob | 17,800 | 8.000 | 96.8 | 3.2 | **96.8** |
| Portsweep | Prob | | | 94,8 | 5.2 | |
| Spy | R2L | 14,700 | 5.000 | 97.8 | 2.2 | **97.7** |
| Stan | R2L | | | 95,9 | 4.1 | |
| Multihop | R2L | | | 97.7 | 2.3 | |
| Normal | Normal | 30.000 | 30.000 | 99.6 | 0.4 | 99.6 |
| **Total Testing Rate** | | | | **97.7** | **1.7** | |

We trained the fuzzy genetic algorithm on testing dataset in which 20% of the NSL-KDD data was taken for this purpose. Each connection record consists of 41 features and labelled in order sequences such as: 1,2,3,4,5,6,7... 41 in addition to the 42$^{nd}$ attribute which is the assigned class; normal or anomaly. These attributes fall into four main categories as in (Mahoney & Chan, 2003), (Tavallaee et al. 2009). We chose 6 types of DoS instances, 4 attack types of Probe instances, and 4 types of R2L attack instances from the training dataset performing five test Cases C1, C2, C3,..,C5 for each category as shown in Table 8. We have tested 14 attack types as well as the normal connections. Considerably, we chose 4 types of the attacks as unknown attacks in the testing dataset in order to test our Fuzzy Genetic Algorithm (FGA). The attack types are; Neptune, Xmas Tree, Multihop, and Spy. Finally, we tested each type of attacks separately to examine and investigate the accuracy and to observe the performance of the detection method. See Table 8 for details of the testing cases results.

**Table 8.** Suggested Five Test Cases To Detect Attacks Using Hidden Channels**.**

| # | Data Type | Category | C1 | C2 | C3 | C4 | C5 |
|---|---|---|---|---|---|---|---|
| **1** | Smurf | DoS | x | | x | | |
| **2** | Pod | DoS | x | | | x | |
| **3** | Teardrop | DoS | x | | | | |
| **4** | Jping | DoS | | x | | | |
| **5** | UDP Flood | DoS | | | x | | x |
| **6** | neptune | DoS | | x | | | x |
| **7** | Ipsweep | Prob | | | | x | |
| **8** | Portsweep | Prob | | x | | | x |
| **9** | Hostscan | Prob | | | | x | |
| **10** | Xmas Tree | Prob | | x | | x | |
| **11** | Spy | R2L | | | x | | |
| **12** | Satan | R2L | | | x | | |
| **13** | ftp_write | R2L | | x | | x | |
| **14** | Multihop | R2L | | | x | | |
| **15** | Normal Status | Normal | | | | | |

## Discussion

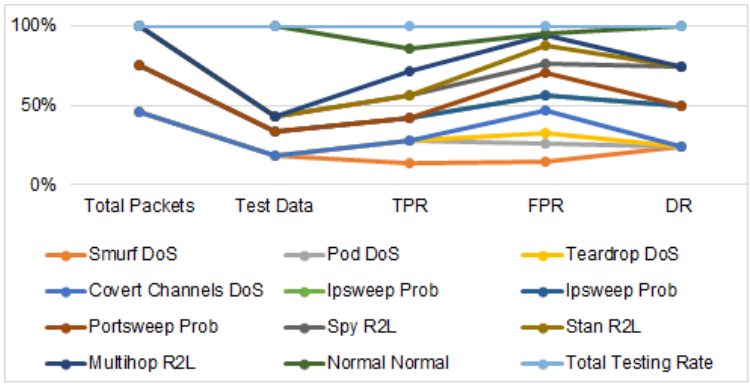
The results of both experiments confirm the initial hypothesis of our suggested Fuzzy Genetic Algorithm (FGA). The performance of the process was impressive with regards to the significant accuracy to each test experiments phases so far. In Table 7 and Figure 5, we observe the distinguished correctness and low false positive of the suggested mechanism.

**Table 9.** Results of Suggested Fuzzy Genetic Algorithm (FGA) Results Using Five Test

| *TC* | Data Type | Nive Bayes DR (%) | Av (%) | FGA DR(%) | Av (%) |
|---|---|---|---|---|---|
| *1* | Neptune | 92.4 | 91.15 | 97.8 | **96.37** |
| | Xmas Tree | 91.7 | | 96.1 | |
| | Multihop | 90.7 | | 93.1 | |
| | Spy | 89.8 | | 98.5 | |
| *2* | Jping | 88.6 | 61.9 | 98.4 | **95.6** |
| | UDP Flood | 28.6 | | 94.8 | |
| | Pod | 68.5 | | 93.6 | |
| *3* | Ipsweep | 55.3 | 64.46 | 94.6 | **94.03** |
| | Portsweep | 93.6 | | 92.4 | |
| | Hostscan | 44.5 | | 95.1 | |
| *4* | Smurf | 95.6 | 91.75 | 90.5 | **90.3** |
| | Satan | 87.9 | | 90.1 | |
| | Teardrop | 67.3 | | 89.9 | **91.65** |
| *5* | ftp_write | 77.3 | 72.3 | 93.4 | |

The test was carried out using our primary data which were generated from two security tools; our security tool written in Python and (THC) tool which was written in C (Hauser, 2015). The testing dataset was taken from the overall training dataset to perform the detection, moreover the accuracy is competitive with an average of 97.7 % of the total testing data and with 96.6 % for the training dataset. To validate the efficiency of the suggested technique, we performed the second experiment with another classification algorithm; Naïve Bayes classifier. Obviously, this step gave us an indication of potential improvement of our suggested approach.

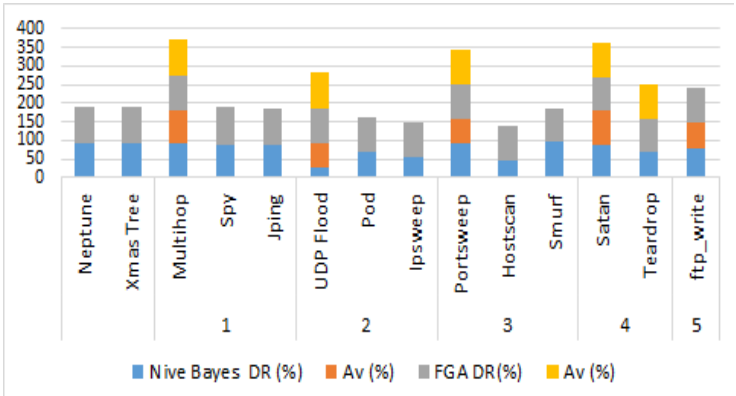
**Fig 5.** Results of Suggested FGA Framework to Detect Covert Channels




To Analyze the results given in Table 9 and the Graph in Figure 6, we compared the outcome (DR) of the Test Cases observing that only one test case (TC4), which we used Naive Bayes classifier was better than FGA. However in test cases TC1, TC2, TC3 and TC5, FGA was improved exclusively and depicted the unknown attacks with the highest accuracy detection rate (DR) by 96.37 %, meanwhile Naïve Bayes algorithm obtained an average of detection rate of 91.15 % in test case 1 with differences of 5.22 %, then in test case 2 Naive Bayes obtained 61.9 % accuracy in detection rate, while the FGA accuracy detection rate was 95.6 % with over 33.7 % differences in DR.

Significantly, Naive Bayesian Algorithm gave a low detection rate in test case 3 with the difference of 29.84 % obtaining 64.46\% accuracy, but FGA obtained in the same test case over 94.03 %. Fuzzy Genetic Algorithm has an overall detection rate with 93.59 % running on NSL-KDD'99 dataset in the second experiment, while getting 97.7 % in the first experiment using our primary generated attack data types.

**Fig 6.** Results of Unknown Attack Detection Testing NSL-KDD Dataset Using Suggested FGA Framework




## 5. CONCLUSION AND FUTURE WORK

Similar to what Fries (2008) and Jongsuebsuk et al. (20013) suggested for TCP/IPv4 attacks, new attempts required to detect storage covert channels and anomaly attacks in TCP/IPv6 using Artificial Intelligence Techniques in respond to the novel vulnerabilities in this protocol. Potentially, this approach should act as a countermeasure restrain to sophisticated attack tools used by hackers. Using Fuzzy Genetic Algorithm to tackle such network threats in IPv6 and ICMPv6 protocols will add a new route of cutting-edge solutions for security systems in the real world. We have answered the project question about the possibility to detect and mitigate unknown and new attacks through covert channels manipulation using Artificial

Intelligence techniques. However approaches in (Supriyanto et al. 2012), Salih et al. (2015), (Liu & Lai, 2009), (Redhwan et al. 2013), (Bahaman et al. 2011) dealing with IPv6 security sophisticated threats have some concerned issues as mentioned in (Salih et al. 2015).

In this paper, we applied an enhanced Fuzzy Genetic Algorithm (FGA) approach to suggest a novel IDS for IPv6/ICMPv6. We implemented a hybrid Genetic and Fuzzy rules due to the fast, flexible and high performance given to detect unknown attacks (Hogue et al. 2012) and covert channels in IPv6. Furthermore we proposed 10 characteristics of different attack instances against this New Generation Internet Protocol. This proposed approach in FGA heterogeneously reduces the probabilistic stimulation, which leads to higher accuracy in detection and classification process, because the Fuzzy Genetic Algorithm is a rule-based, consequently leads to less computation time, lower false negative rate (FNR) and higher true positive rate (TPR) in comparison to other tested MLA techniques.

Future work will focus on the MITM attack detection to examine the certainty and specificity of the features selected in the primary dataset. Aiming to use an enhanced Support Vector Machine (SVM) in a supervised learning approach and compare it against our current approach to see the efficiency and the performance of both methodologies. However an SVM can only identify simple features (Sohn et al. 2003), it's unlikely to detect complex values in IPv6 header fields and the embedded (Wendzel et al. 2015) inter-dependencies without other advanced techniques. This will reduce and eliminate partially the unauthorized access and its side effects on classified data communication using IPv6.

## REFERENCES


Bahaman, N., Anton Satria, P., & Mas' ud, Z. (2011). Implementation of IPv6 network testbed: Intrusion detection system on transition mechanism. *Journal of Applied Sciences*, *11*(1), 118-124.

Chen, S. H., Jakeman, A. J., & Norton, J. P. (2008). Artificial intelligence techniques: an introduction to their use for modelling environmental systems. *Mathematics and Computers in Simulation*, *78*(2), 379-400.

Choudhary, A. R. (2009, November). In-depth analysis of IPv6 security posture. In *2009 5th International Conference on Collaborative Computing: Networking, Applications and Worksharing*.

Fries, T. P. (2008, July). A fuzzy-genetic approach to network intrusion detection. In *Proceedings of the 10th annual conference companion on Genetic and evolutionary computation* (pp. 2141-2146). ACM.

Gomez, J., & Dasgupta, D. (2002, June). Evolving fuzzy classifiers for intrusion detection. In *Proceedings of the 2002 IEEE Workshop on Information Assurance* (Vol. 6, No. 3, pp. 321-323). New York: IEEE Computer Press.

Hoque, M. S., Mukit, M., Bikas, M., & Naser, A. (2012). An implementation of intrusion detection system using genetic algorithm. ArXiv preprint arXiv: 1204.1336.

Jongsuebsuk, P., Wattanapongsakorn, N., & Charnsripinyo, C. (2013, January). Network intrusion detection with Fuzzy Genetic Algorithm for unknown attacks. In *Information Networking (ICOIN), 2013 International Conference on* (pp. 1-5). IEEE.

Liu, Z., & Lai, Y. (2009). A data mining framework for building intrusion detection models based on IPv6. In *Advances in Information Security and Assurance* (pp. 608-618). Springer Berlin Heidelberg.

Mahoney, M. V., & Chan, P. K. (2003, September). An analysis of the 1999 DARPA/Lincoln Laboratory evaluation data for network anomaly detection. In*Recent Advances in Intrusion Detection* (pp. 220-237). Springer Berlin Heidelberg.

Marc, Hauser. (2013)."IPv6 Security Vulnerabilities" Available https://www.thc.org/thc-ipv6 . Accessed 10 Feb 2016.

Martin, C. E., & Dunn, J. H. (2007, October). Internet Protocol version 6 (IPv6) protocol security assessment. In *Military Communications Conference, 2007. MILCOM 2007. IEEE* (pp. 1-7). IEEE.

Redhwan. M. A. Saad, Slevakumar Manickam, Ramadass, S. (2013) Intrusion Detection System in IPv6 Network Based on Data Mining Techniques–Survey. Proc. of 2nd International Conference on Advances in Computer and Information Technology ACIT 2013.Malaysia.

Salih, A., Ma, X., & Peytchev, E. (2015). Detection and Classification of Covert Channels in IPv6 Using Enhanced Machine Learning. Proc of the International Conference on Computer Technology and Information Systems. (ICCTIS) N & N Global Technology DUBAI, UAE, 2015.

Salih, A., Xiaoqi Ma, and Evtim Peytchev. (2015) "New Intelligent Heuristic Algorithm to Mitigate Security Vulnerabilities in IPv6", International Journal for Information Security (IJIS), Volume 4, DOI: 04.IJIS.2015.

Sohn, T., Seo, J., & Moon, J. (2003, October). A study on the covert channel detection of TCP/IP header using support vector machine. In *ICICS* (pp. 313-324).

Supriyanto, Hasbullah, I. H., Murugesan, R. K., & Ramadass, S. (2013). Survey of internet protocol version 6 link local communication security vulnerability and mitigation methods. IETE Technical Review, 30(1), 64-71.

Tavallaee, M., Bagheri, E., Lu, W., & Ghorbani, A. A. (2009). A detailed analysis of the KDD CUP 99 data set. In *Proceedings of the Second IEEE Symposium on Computational Intelligence for Security and Defense Applications 2009*.

Vivek, T. K., & Kalimuthu, M. Improving Intrusion Detection Method for Covert Channel in TCP/IP Network. International Journal of Computer Science Trends and Technology (IJCST), vol.2, no. 2, March. 2014.

Wendzel, S., Zander, S., Fechner, B., & Herdin, C. (2015). Pattern-based survey and categorization of network covert channel techniques. *ACM Computing Surveys (CSUR), 47*(3), 50.

Zander, S., Armitage, G., & Branch, P. (2006, December). Covert channels in the IP time to live field. In *Proceedings of Australian Telecommunication Networks and Applications Conference (ATNAC)*.