ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A Novel Anonymity Prevention Technique in Attacks with Unsupervised Learning Model

Ch.Sneha[1],J.Vasudeva Rao[2],D.Dharmaiah[3]

[1]PG Scholar, Dept. of CSE, Vignan's Institute of Information Technology, Visakhapatnam, India

[2]Asst Professor, Dept. of CSE, Vignan's Institute of Information Technology, Visakhapatnam, India

[3]Professor, Dept. of CSE, Vignan's Institute of Information Technology, Visakhapatnam, India

ABSTRACT*:* With the tremendous growth of network-based services and sensitive information on networks, network security is getting more and more importance than ever. Networks are particularly vulnerable to several key types of attacks. Attacks can be performed in a variety of ways, most notably as denial of service attacks, but also through traffic analysis, privacy violation, and physical attacks and so on. They can disturb remote transmission and can happen either inadvertently as commotion or obstruction at the recipient side. So it is essential to detect an anomaly node in the network. In this paper, we are proposing a novel approach for the detection of anonymous node with Naive Bayesian classification. It identifies and analyzes the behavior of the incoming node by computing the posterior probability of the incoming node with training data set at receiver end and adds to node list if not anonymous. And this model comes under unsupervised learning model (in terms of machine learning and data mining). Training data set can be taken with parameters of source IP, destination IP, port number, number of packets transmitted and type of protocol. Receiver node need not analyze the behavior of incoming node for every request because once it is added to node list it is treated as genuine node. We are using Triple DES (Data Encryption Standard) algorithm for secure transmission of data between genuine nodes, it encodes the data packets at sender end and decodes at receiver end.Triple Data Encryption Algorithm (TDEA or Triple DEA) key block, which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Triple DES provides a relatively simple method of increasing the key size of DES to protect against any attacks, without the need to design a completely new block cipher algorithm.

KEYWORDS: Jamming attacks; Anonymous node; Naive Bayesian classification; 3DES encryption.

I. INTRODUCTION

The terms Network Security and Information Security are often used interchangeably. Network Security is generally taken as providing protection at the boundaries of an organization by keeping out intruders (hackers). Information Security, however, explicitly focuses on protecting data resources from malware attack. Network security starts from authenticating any user, commonly (one factor authentication) with a username and a password (something you know). With two factor authentication something you have is also used (e.g. a security token, an ATM card, or your mobile phone), or with three factor authentication something you are also used (e.g. a fingerprint or retinal scan). Once authenticated, a statefulfirewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component fails to check potentially harmful content such as computer worms being transmitted over the network.

An intrusion prevention system helps to detect and inhibit the action of such malware [2]. An anomaly-based intrusion detection system also monitors network traffic for suspicious content, unexpected traffic and other anomalies to protect the network e.g. from denial of service attacks.Communication between two hosts using the network could be encrypted to maintain privacy[1][4].

DOI: 10.15680/IJIRCCE.2015. 0311076

Remote innovations have turned out to be progressively prominent in our ordinary business and individual lives. It empowers one or more gadgets to convey without physical associations without requiring system or fringe cabling. As we realize that remote systems serve as the vehicle instrument in the middle of gadgets and among gadgets, on the other hand, in view of this remote nature these are inclined to various security dangers in which one of the major genuine security risks is jamming [7].

A malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called jamming and the malicious nodes are referred to as jammers. Jamming techniques vary from simple ones based on the continual transmission of interference signals, to more sophisticated attacks that aim at exploiting vulnerabilities of the particular protocol used [9]. Jamming attacks come under DoS(Denial of service) attacks. DoS attack is a critical component of any security system as these attacks can affect theavailability of a node or an entire network [1]. Even though there are numerous ways to secure a network and protect the network from numerous attacks, detecting an anonymous node is a big challenge.

In this paper, we are proposing a novel approach for detection and prevention of attacks using Naïve Bayesian classification. Naive Bayes is one of the most efficient and effective Inductive learning algorithms for machine learning and data mining. It uses unsupervised learning model approach to find whether the behavior of incoming node is anomaly or not. Preparation of dataset which comprises of source IP address or name, Destination IP address and port number, kind of convention and number of bundles transmitted from source to destination. When a node unites with another node, at that time a testing sample is formed. Both the training dataset and testing dataset are sent to Naïve Bayesian classifier, where it initially computes the maximum similarity with the centroids of the clusters and places the input record with respect to cluster holder and then computes the probability of anomaly status (i.e. positive and negative probability).

When the incoming node is detected as a non-anonymous node, the data is transmitted between the nodes using 3DES (data encryption standard),a mode of the DES encryption algorithmthat encrypts data three times [6]. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key). In this way, anonymous node is detected an anonymous transmission is prevented. Therefore communication takes only between genuine nodes and confidentiality of the transmitted message is ensured.

II. Related work

The system comprises of an accumulation of nodes joined by means of remote connections. Nodes may convey straightforwardly on the off chance that they are inside of correspondence reach, or in a roundabout way by means of various bounces. Nodes convey both in unicast mode and show mode. Correspondences can be either decoded or encoded. For scrambled show correspondences, symmetric keys are shared among every planned beneficiary and these keys are built up utilizing pre-shared pair wise keys or topsy-turvy cryptography.

Packets are transmitted at a rate of R bauds. Each PHY-layer image relates to q bits, where the estimation of q is characterized by the fundamental advanced adjustment plan. Each image conveys αβ q information bits, where α/β is the rate of the PHY-layer encoder. Here, the transmission bit rate is equivalent to q^R bps and the data bit rate is αβ q^R bps. Spread range (SS) strategies, for example, recurrence bouncing spread range (FHSS), or direct grouping spread range (DSSS) may be utilized at the PHY

-layer to shield remote transmissions from sticking. SS gives invulnerability to impedance to some degree (regularly 20 to 30 dB pick up), however an effective jammer is still fit for sticking information bundles of his choosing.

Adversary Model– We expect the foe is in control of the correspondence medium and can stick messages at any piece of the system of his picking. The enemy can work in full-duplex mode, in this manner having the capacity to get and transmit all the while. This can be accomplished, for instance, with the utilization of multi-radio handsets.

Here the contribution towards jamming attacks is reduced by using the two algorithms: 1) Symmetric encryption algorithm 2) Brute force attacks against block encryption algorithms. The proposed algorithm keeps these two in mind as they are essential in reducing the jamming attacks by using the packet hiding mechanism. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack [3]. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. For example, a jammer can target route- request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow to launch selective jamming attacks, the adversary must be capable of implementing a classify-then-jam strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifyingtransmittedpackets using protocol semantics, or by decoding Packets on the transfer.

III.PROPOSED ALGORITHM

In our work, in data exchange systems or network systems, authenticated user finding is achieved based on the classification of the users. In this method, we will find the user is anonymous or not anonymous at the time of getting in to the network. The process is explained below.

We are proposing a proficient firewall information order over log information or preparing dataset which comprises of source IP address or name, Destination IP address and port number, kind of convention and number of bundles/packets transmitted from source to destination. Initially the sender and receiver nodes should login and browse for dataset and select the input dataset. Then, the source node should add the details of the receiver node (such as node IP, port no. and content to be transmitted) in order to transmit message to the receiver. At the point when a node unites it recovers the meta-information i.e. testing dataset and advances to the preparation dataset. Both preparing and testing datasets can be sent to NAIVE BAYESIAN classifier for breaking down the conduct of the joined node [5]. Hence at the source node only, Naïve Bayesian is analyzing the behavior of the node and adds the node only if it is a non-anonymous node. In this way a genuine node is added to the node list, we need not analyze the node for every request. This also helps in improving the performance of system.

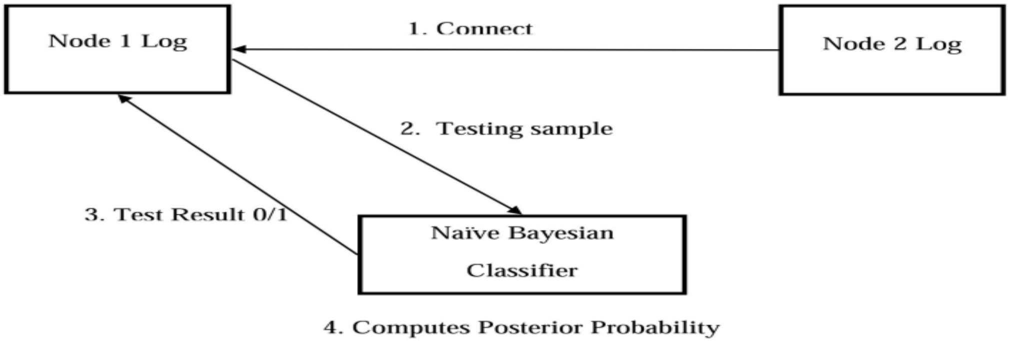


Fig.1.System Architecture

The system architecture and architectural components are clearly shown in Fig.1. For optimal performance, it classifies input node with suitable cluster data instead on entire dataset. Initially it computes the probability of anomaly status (i.e. positive and negative probability).The process of detectinganomoly node by the unsupervised approach of Naive bayes classifier is shown in the system architecture. Only the genuine nodes communicate by 3DES encryption scheme.

Naive Bayesian Classification
Algorithm to classify malicious agent
Sample space: set of agent
H= Hypothesis that X is a node
P (H/X_i) is our confidence that X_i is an incoming node
P(H) is Prior Probability of H and it is probability that any given training sample is an agent regardless of its anomaly or not anomaly behavior

DOI: 10.15680/IJIRCCE.2015. 0311076

P(H/X) is a conditional probability and P(H) is independent of X
Estimating probabilities:
P(H), P(X_i) and P(X_i/H) may be estimated from given training and testing data samples
P(H|X_i)=P(X_i|H)*P(H)/P(X_i)

Steps involved:
1. Each training data sample is of attribute type
X= (x_j) j =1(1….n), where x_j is the values of X for attribute A_j
2. Suppose there are m decision classes C_j, j=1(1…m).
P(C_i|X) > P(C_j|X) for 1<= j <= m, j>i
i.e. classifier assigns X to decision class C_j having highest posterior probability conditioned on testing sample X
The decision class for which P(C_j|X) is maximum is known as maximum posterior hypothesis of the sample.
From Bayes Theorem
3. P(X_i) is constant and Only need be maximized.

- if class initial probabilities not known prior then we can assume all decision classes to be more equally likely decision classes
- Otherwise maximize the samples P(C_i) = Si/S

4. Naïve assumption for attribute independence
P(X|C_j) = P(x_1,…..,x_m|C) = PP(x_k|C)
5. To classify an unknown testing sample X_i, compute each decision class $C_i$and Sample X is assigned to the class
iff (Prob(X_i|C_i)P(C_i)> P(X_i|C_j) P(C_j)).

In our methodology, we propose a productive characterization based methodology for breaking down the unknown clients over system activity and computes the trust measures in terms of the preparation information with the secret testing information. Our design contributes with the accompanying modules like Analysis specialist, Neighborhood node, Classifier, Information gathering and preprocessing.

Investigation Agent –Analysis operators or Home Agent is available in the framework and it screens its own particular framework persistently. In the event that an assailant sends any packet to accumulate data or telecast through this framework, it calls the classifier development to figure out the assaults. In the event that an assault has been made, it will channel the particular framework from the worldwide system.

Adjoining node - Any framework in the system exchange any data to some other framework, it telecast through moderate framework. Before it exchanges the message, it sends portable operators to the neighboring node and accumulates all the data. It returns back to the framework and it gets classifier standard to figure out the assaults. In the event that there is no suspicious action, it will forward the message to neighboring node.

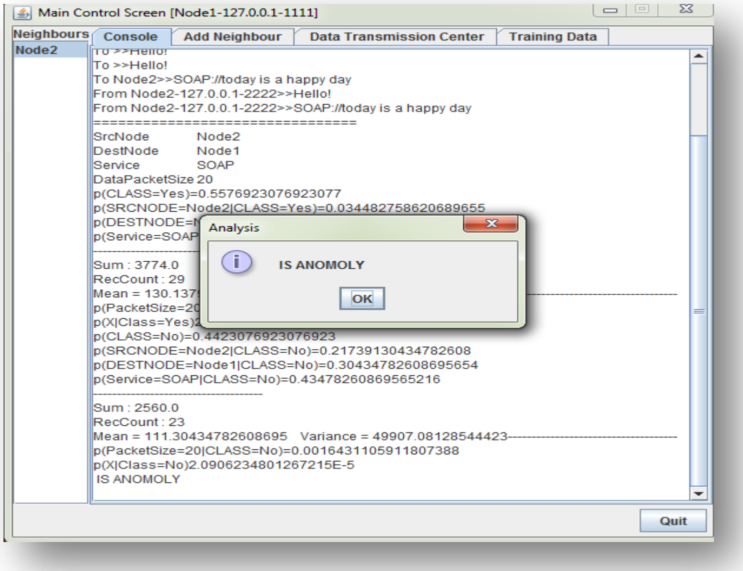
Data Collection: Information collecting module is incorporated for every peculiarity location subsystem to gather the estimations of elements for relating layer in a framework. Typical profile is made utilizing the information gathered amid the ordinary situation. Assault information is gathered amid the assault situation.

The review information is gathered in a record and it is smoothed so that it can be utilized for inconsistency location. Information pre-procedure is a strategy to transform the data with the test training information. In the whole layer irregularity recognition frameworks, aforementioned pre-preparing system is utilized for the order process we are utilizing Naive Bayesian classifier for breaking down the neighbor node testing information with the preparation information.

IV.RESULTS

For experimental analysis we used networking programming model for node connectivity in java programming language through sockets. We have used a synthetic dataset which contains the parameters like source IP or name, destination IP or name, type of protocol and packets transmitted. Our experimental analysis analyzes the node anonymity of positive chances and negative chance of probability instead of stating the class.

There are two cases in this scenario. They are:
Case 1: When the incoming node is detected asan "anomoly"
Case 2: When the incoming node is detected asa "non-anomoly"

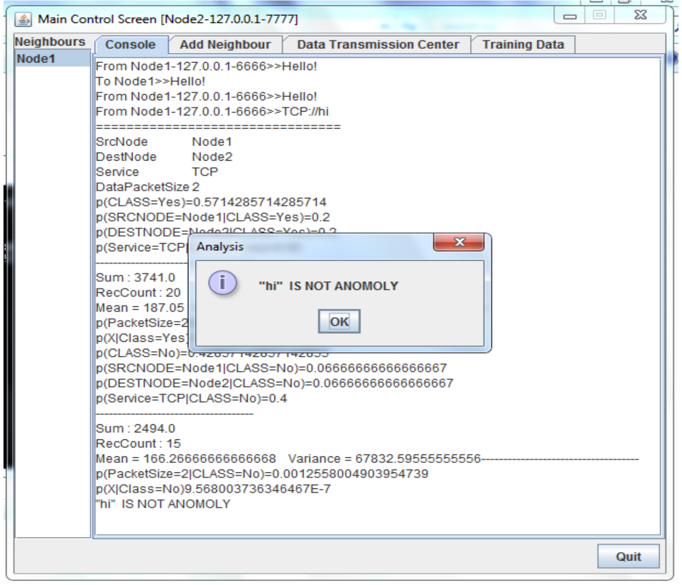


```
To >>Hello!
To >>Hello!
To Node2>>SOAP://today is a happy day
From Node2-127.0.0.1-2222>>Hello!
From Node2-127.0.0.1-2222>>SOAP://today is a happy day
================================
SrcNode         Node2
DestNode        Node1
Service         SOAP
DataPacketSize 20
p(CLASS=Yes)=0.5576923076923077
p(SRCNODE=Node2|CLASS=Yes)=0.034482758620689655
p(DESTNODE=N
p(Service=SOAP
--------------------
Sum : 3774.0
RecCount : 29
Mean = 130.137                                       ----------------------------
p(PacketSize=20
p(X|Class=Yes)2
p(CLASS=No)=0.4423076923076923
p(SRCNODE=Node2|CLASS=No)=0.21739130434782608
p(DESTNODE=Node1|CLASS=No)=0.30434782608695654
p(Service=SOAP|CLASS=No)=0.43478260869565216
----------------------------------
Sum : 2560.0
RecCount : 23
Mean = 111.30434782608695   Variance = 49907.08128544423-----------------------------
p(PacketSize=20|CLASS=No)=0.001643110591180738‌8
p(X|Class=No)2.0906234801267215E-5
 IS ANOMOLY
```

IS ANOMOLY

Fig.2. The Incoming Node is detected as an "anomoly" node

In Fig.2, we can see the working of the Naive bayes classifier in detecting the incoming node behavior as an anomoly node which indicates that the attack has been occurred.When the incoming node is detected as an anomoly node then the data transmission cannot take place. This is also very helpful in detection of jamming attacks.

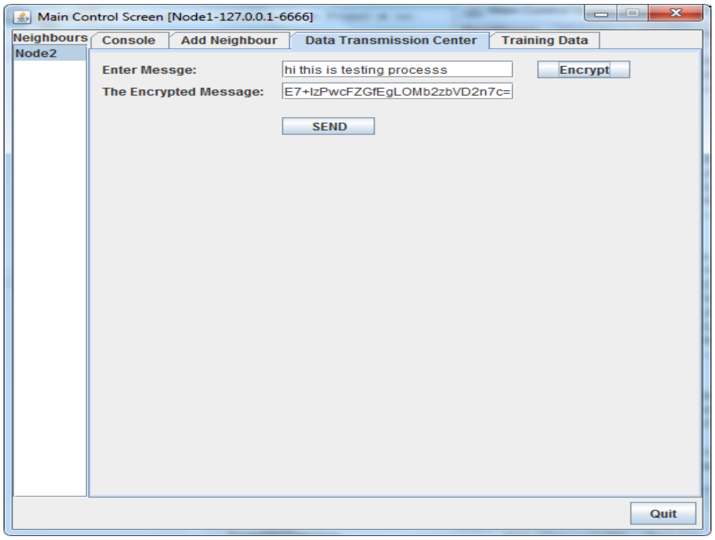


```
From Node1-127.0.0.1-6666>>Hello!
To Node1>>Hello!
From Node1-127.0.0.1-6666>>Hello!
From Node1-127.0.0.1-6666>>TCP://hi
================================
SrcNode         Node1
DestNode        Node2
Service         TCP
DataPacketSize 2
p(CLASS=Yes)=0.5714285714285714
p(SRCNODE=Node1|CLASS=Yes)=0.2
p(DESTNODE=
p(Service=TCP
--------------------
Sum : 3741.0
RecCount : 20
Mean = 187.05
p(PacketSize=2
p(X|Class=Yes)
p(CLASS=No)=
p(SRCNODE=Node1|CLASS=No)=0.06666666666666667
p(DESTNODE=Node2|CLASS=No)=0.06666666666666667
p(Service=TCP|CLASS=No)=0.4
----------------------------------
Sum : 2494.0
RecCount : 15
Mean = 166.26666666666668   Variance = 67832.59555555556-----------------------------
p(PacketSize=2|CLASS=No)=0.0012558004903954739
p(X|Class=No)9.568003736346467E-7
"hi"  IS NOT ANOMOLY
```

"hi" IS NOT ANOMOLY

Fig.3.The incoming node is detected as "not an anomoly" node.

In Fig.3,we can see the working of the Naive bayes classifier in detecting the incoming node behavior as a non-anomoly node.When the incoming node is detected as “not anomoly” node, then the data transmission takes place using 3DES (Data Encryption Standard) cryptographic scheme which is depicted in Fig.4.

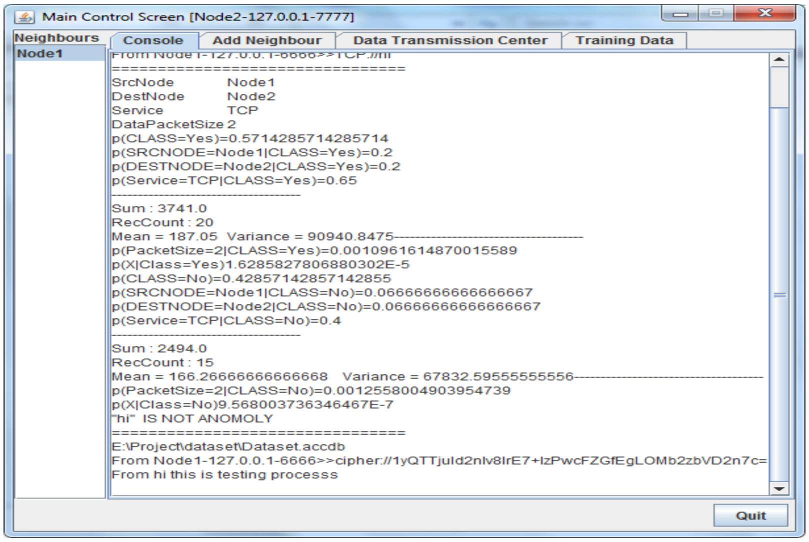


Enter Messge: hi this is testing processs

The Encrypted Message: E7+IzPwcFZGfEgLOMb2zbVD2n7c=

Fig.4. Data transmission using 3DES scheme

Now the sender can transmit the data to the receiver by entering the message in the respective field.For the anonymity prevention, here we are using 3DES encryption scheme.When the sender clicks on Encrypt button, the message is encrypted by the working mechanism of 3DES encryption scheme.The sender clicks on Send button after the message is encrypted. This process is shown in Fig.4.



```
From Node1-127.0.0.1-6666>>TCP://hi
================================
SrcNode         Node1
DestNode        Node2
Service         TCP
DataPacketSize 2
p(CLASS=Yes)=0.5714285714285714
p(SRCNODE=Node1|CLASS=Yes)=0.2
p(DESTNODE=Node2|CLASS=Yes)=0.2
p(Service=TCP|CLASS=Yes)=0.65
--------------------------------
Sum : 3741.0
RecCount : 20
Mean = 187.05  Variance = 90940.8475--------------------------------
p(PacketSize=2|CLASS=Yes)=0.0010961614870015589
p(X|Class=Yes)1.6285827806880302E-5
p(CLASS=No)=0.42857142857142855
p(SRCNODE=Node1|CLASS=No)=0.06666666666666667
p(DESTNODE=Node2|CLASS=No)=0.06666666666666667
p(Service=TCP|CLASS=No)=0.4
--------------------------------
Sum : 2494.0
RecCount : 15
Mean = 166.26666666666668   Variance = 67832.59555555556--------------------------------
p(PacketSize=2|CLASS=No)=0.0012558004903954739
p(X|Class=No)9.568003736346467E-7
"hi"  IS NOT ANOMOLY
================================
E:\Project\dataset\Dataset.accdb
From Node1-127.0.0.1-6666>>cipher://1yQTTjuId2nIv8IrE7+IzPwcFZGfEgLOMb2zbVD2n7c=
From hi this is testing processs
```

Fig.5. Data Transmission result

In Fig.5,we can see the data being transmitted from the source node to Destination node.It shows that the data packet or message is successfully transmitted. The algorithmic implementation and in&out process details are shown in console.

Communication between the genuine nodes is carried out by 3DES cryptographic scheme, a mode of the DES encryption algorithmthat encrypts data three times. The procedure for decrypting something is the same as the procedure for encryption, except it is executed in reverse. Three 64-bit keys are used, instead of one, for an overall key length of 192 bits (the first encryption is encrypted with second key, and the resulting cipher text is again encrypted with a third key)[8]. Data Confidentiality can be ensured by using 3DES. In this way attacks can be prevented.

V. Conclusion

The disadvantages of existing system are analyzedwith parameters like the packet data, payload and other header information which failed in giving an inaccurate result of anonymous behavior.

We are concluding our research work with efficient classification approach (Naive Bayesian algorithm) by analyzing the anonymous behaviors of the log data packet analysis with their respective posterior probabilities of the individual attribute and final class labels to compute final probabilities of the connected node. Data Confidentiality is ensured by using 3DES cryptographic scheme. In this way only genuine nodes can be efficiently communicated with each other and there is no way for anonymous node communication or to increase traffic.

References

[1] A.D. Wood and J.A.Stankovic, “Denial of Service in Sensor networks”, computer, Vol.35,Issue 10, pp. 54-62, 2002.

[2] P.Kavitha and M.Usha, “Anomaly based intrusion detection in wlan using discrimination algorithm combined with naive Bayesian classifier”,Journal of Theoretical and Applied Information Technology,Vol. 61,Issue3, pp.646-653, 2014.

[3] W.Xu, W.Trappe, Y.Zhang and T.wood, “The feasibility of launching and detecting jamming attacks in wireless networks”, in proceedings of MobiHoc, pp. 46-57, 2005.

[4] Mrutyunjaya Panda and ManasRanjanPatra, “Network intrusion detection using naive bayes”, International Journal of Computer Science(IJCSNS) and Network Security, Vol. 7, Issue 12, 2007.

[5] Aniket.P.Sagane and Prof.S.S.Dhande, “Malicious Code Detection Using NaïveBayes Classifier”,International Journal of Application or Innovation in Engineering & Management (IJAIEM),Vol. 3, Issue 4, 2014.

[6] S.Karthik and A. Muruganandam, “Data Encryption and Decryption by Using Triple DES and Performance Analysis of Crypto System”,International Journal of Scientific Engineering and Research (IJSER), Vol. 2, Issue 11, 2014.

[7] P.Mohanraj and A.Mummoorthy, “Use of Jammer network to detect denial of services attack in wireless network”, International Journal of Game Theory and Technology (IJGTT), Vol. 2, Issue 1/2, 2014.

[8] Sombir Singh, Sunil K. Maakar and Dr.Sudesh Kumar, “Enhancing the Security of DES Algorithm using Transposition Cryptography Techniques”,International Journal of Advanced Research in Computer Science and Software Engineering(IJARCSSE),Vol. 3, Issue 6, 2013.

[9] Ali Hamieh and Jalel Ben-Othman, “Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution”, IEEE ICC 2009 proceedings, 2009.

DOI: 10.15680/IJIRCCE.2015. 0311076