Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 50 (2015) 109 – 114

Procedia Computer Science

2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Fuzzy Based Intrusion Detection Systems in MANET

Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G

School of Information and Technology, VIT University - Vellore Campus, Tamilnadu, India

E-mail: vishnubalan91@gmail.com, priyanit085@gmail.com, gokulkapoor@gmail.com, ushadevi.g@vit.ac.in

Abstract

Mobile adhoc network (MANET) is an infrastructure less wireless network and self-organized. During communication mobile adhoc network do not use any proper infrastructure so that MANET initiates request for data transfer, so MANET is vulnerable to various type of attacks such as black hole attack, warm hole attack, gray hole attack. The proposed system is to detect the malicious behavior of node by intrusion detection system with fuzzy logic technique and also to identify the type of attacks. The system is robust enough to detect attacks such as black hole attack and gray hole attack and also able to prevent those kind of attacks by using efficient node blocking mechanism such that the proposed system provides a secure communication between nodes

© 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)

Keywords: mobile adhoc network (MANET);fuzzy logic technique;black hole attack;gray hole attack;

1 INTRODUCTION

In recent years, mobile adhoc networks (MANET) are flexible to various types of application because of its flexibility. There is no fixed infrastructure for MANET, so this facility makes mobile adhoc networks very effective for military application. Each node requests nearby node by using various routing protocols such as AODV, DSR and OLSR to transfer data from one node to another node. But MANET is vulnerable to various types of attacks because of its feature such as communication via wireless links, resource constraints, and dynamic topology.

Many intrusion detection system (IDS) have been developed for MANET to detect various types of attacks, IDS plays crucial role in MANET to detect any type of attacks. An IDS is a software system that is used to analyse misbehaviour and violation of policy, then generate report based on this. Basically intrusion detection system is classified into three types, they are signature based detection, anomaly based detection and specification based detection. The signature based detection compares the signature of existing patterns with network pattern, if any existing attack pattern matches with network pattern then the network is attacked. The anomaly detection is further classified into statistical based, knowledge based and learning based. The anomaly detection considers the normal behavior of networks and also flag the unknown activity, based on this it generates alarm.

2 LITERATURE SURVEY

Recent research in MANET is to detect and prevent the specific attack in the network. Kurosawa and Jamalipour (2007) proposed a mechanism for black hole detection for AODV. Fuzzy based genetic algorithm has been proposed by Wang Yunwu (2009) which uses initial rules from fuzzy algorithm and final rules from genetic algorithm. Genetic based intrusion detection system for TCP/IP networks has been proposed by Wei li (2010).Yi et al (2005) considered RREQ flooding attack, so they invented a new mechanism to prevent RREQ flooding attacks based on the next node supervision. Hu et al (2003) experimented how an attacker can use a rushing attack in the network in DSR and implemented a new method for rushin attack prevention mechanism for MANET. Though many analysts were trying to prevent the network from the attack, some researchers were suggested with general approach. Jungwan Kim et al (2001) proposed the artificial immune system for IDS and it is based on hierarchical approach which is inspired by human immune system. A same approach, Ariadne has proposed a mechanism for end-to-end delivery based on the key that has been shared. More effort is needed to prevent the network from attack. Mechanism proposed in above method is to protect network against other attacker through routing.

1877-0509 © 2015 The Authors. Published by Elsevier B.V. This is an open access article under the CC BY-NC-ND license (http://creativecommons.org/licenses/by-nc-nd/4.0/).

Peer-review under responsibility of scientific committee of 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15)
doi:10.1016/j.procs.2015.04.071

The intelligent based intrusion detection systems is used I network to find the intruder node using attributes. Similarly IAWDO and IAMSV method were proposed to detect the intruder in distributed environment that use of trust in transactions. Energy Based Trust Solution System finds a node whether it's an intruder's node or not depending on the trusties has four components to find the intruder node. They are 1. Supervisor module 2. Aggregator module 3. Trust calculator module and 4.Disseminator module. The supervisor module will supervise the next node using Passive acknowledgement (PACK). PACK is used to detect whether nodes are forwarded to correct node or not, by supervising their communications. Based on the communication, if there is any difference in the nodes then the aggregator component does it work.

3 PROPOSED METHOD

The proposed system consists of three main blocks: they are attack categorization, fuzzy implementation and fuzzy estimation.

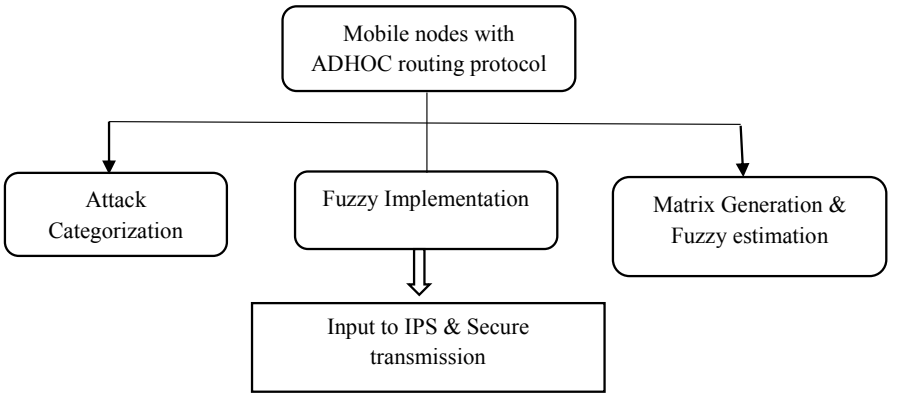

Figure 1 System Architecture

3.1 Attack categorization

The MANET attacks are broadly classified into two types [Revathi et al, 2012], they are external attacks and internal attacks. The internal attack is performed by compromised node belongs to the same network. The external routing is initiated by outside source which replay false routing information or old routing information to increase the network overload. The proposed system mainly suitable for two attacks such as black hole attack and gray hole attack

3.1.1 Gray hole attack

This attack leads to dropping of packets. The attacking node initially behaves correctly and reply correct route reply message to node which initiates the RREQ message. Afterwards the node fails to forward the packet which leads to dropping of packets, then the network get damage. In any case the node always try to find exact route information which makes the particular node to consume more energy and therefore this attack leads to dropping of packets and consume its battery more. If the gray hole present near source node then it is gray hole towards source and similarly if the gray hole present near the destination then it is gray hole towards destination.

3.1.2 Black hole attack

Black hole is similar to gray hole attack but in black hole attack the malicious node never send the initial route message correctly as like in gray hole attack, rather it waits for neighbour RREQ message. If the attacker node receives the RREQ message from neighbour then it sends false routing RREP with highest sequence number to neighbour node before the correct RREP reach the neighbour. So the neighbour thought the false RREP is the correct one and send the message by using the false information. So the data packet never reaches the destination properly. Similarly the attacker node attacks all RREQ messages. To succeed in this attack the malicious node should present in the centre of the network.

Gray hole attack one or two nodes to isolate the network whereas the black hole attack affects the entire network. This module categorizes the type of attack and sends information to next fuzzy implementation module.

3.2 Fuzzy implementation module

Fuzzy logic uses various measures of number of packets dropped against various parameters. The fuzzy techniques overcome the problem which was not solved by existing techniques. The fuzzy logic technique is very easy to implement and produce precise output by removing various ambiguities. Since three attacks are used in this paper, three measures are used to calculate fuzzy

values and the measures are named as m1 which indicates the number of packets dropped by node is greater than threshold T, m2 which indicates the number of packets dropped by particular node which is located near destination node is greater than T1 and less than T, and m3 which indicates the number of packets dropped by particular node which is present near source node is greater than T1 and less than T.

The threshold values are choosing based on the behaviour of the network and attacks. The black hole attacker node will drop all packets, so in this paper the threshold value is assumed to be 20% of total packets. The threshold value for gray hole attack is less than the threshold value of black hole attack, hence the threshold value is 5% of total packet. M as the universal set of all the measures M= {m1, m2, m3} and P denotes the universal set of all misbehaviour and attacks P= {p1, p2, p3}. L denotes the nodes which are participating in the topology which is defined as L= {1, 2, 3...l}, where l denotes the number of nodes.

The relation matrix is calculated by L, M, X and this matrix represents the L occurrence with respect to measure M. RS = L X M, where μRs (l, m) (l E L, m EM). This matrix defines the range of m in node l. The matrix RO is calculated by using M, X, P where the matrix represents occurrence relation matrix and M occurrence frequency with respect to attacks P. RO = M X P ,where μRs(m,p)(m E M, p E P). The matrix RC is calculated by using M X P, and this matrix represents the occurrence of M with respect to the attacks P, μRs(m, p)(m E M, p E P)

3.3 Fuzzy estimation

Fuzzy estimation is done based on the value of matrices RS, R1, R2, R3 and R4. Based on the threshold value T and T1, the matrices values are calculated. Consider the matrix RS, the value of matrix is calculated by using the node number and corresponding member function value and denoted by RS[node number][member function value]. The member function value is calculated by using trapezoidal membership method.

Membership value = (x-a)/ (b-a)

Where x=threshold value, a = number of packets forwarded, b = number of packets dropped.

The R0 and RC are assumed depending on the previous value

$$R0 = \begin{pmatrix} 1 & 0.5 & 0.5 \\ 0.5 & 1 & 0.5 \\ 0.5 & 0.5 & 1 \end{pmatrix} \qquad R1 = \begin{pmatrix} 1 & 0.5 & 0.5 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

The RS value is calculated based membership value and updated in the table. Based on this RS value, the remaining value of R1, R2, R3 and R4 are calculated and updated in the table.

I. occurrence indication R1 = RS*R0 (the operator * indicates the max min composition of RS and R0), II. Conformability indication R2 = RS * RC, III. Non-occurrence indication R3 = RS * (1-R0), 1V. Non-symptom indication R4 = (1-RS) * R0

4 IPS MECHANISMS

The IPS gets input from the fuzzy technique and it categorizes the range of attack. If a malicious node is node is detected, then IPS mechanism is activated by setting the node against malicious node. The IPS mechanism changes the path of data packet once the malicious node is detected; this is done by AODV which modifies the path in order to provide secure data communicatio

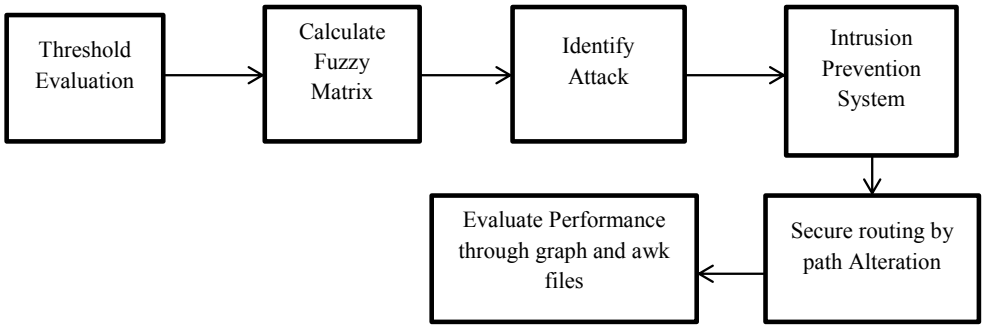

Figure 2 Flow Diagram of IPS Mechanism

The Figure 3 clearly shows the IPS mechanism and this can be done by attacking the malicious node using the node index and increase the network jam for the packet flow of particular node and uses the alternate path.

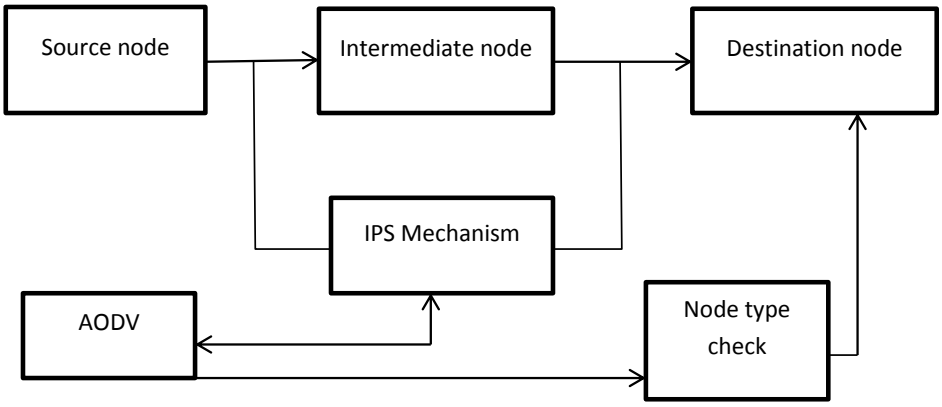

Figure 3 Intrusion prevention system

This mechanism provides an efficient and stable throughput. The IPS is located between the sender and receiver as shown in Figure 4. If any node type matches the gray hole or black hole attack then AODV block the particular node and choose alternate path

5 RESULTS

The performance of the network is tested using network simulator 2 under three condition such as non-attack, black hole attack and gray hole attack. Three performance metrics are used to evaluate the performance such as packet delivery ratio based on entropy variation, throughput based on entropy variation and jitter.

Source Node Intermediate Node Destination Node IPS Mechanism AODV Node type Check

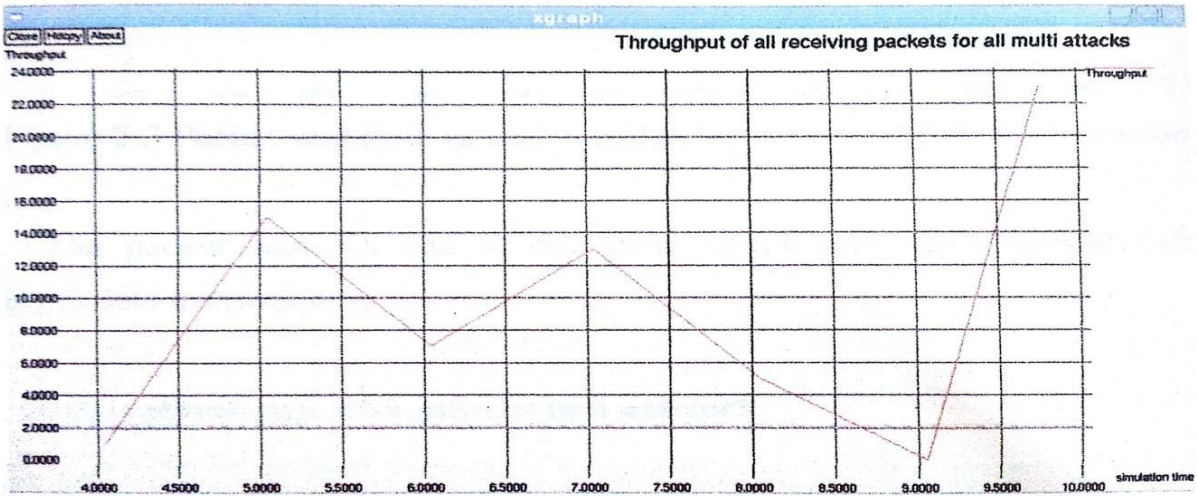

Figure 4 Throughput of receiving packets with black hole and gray hole attack

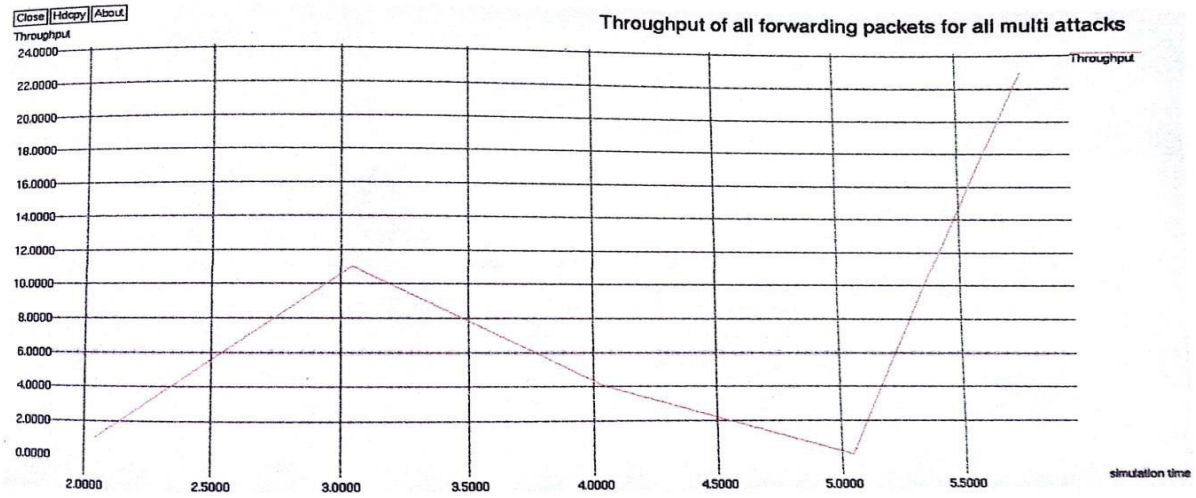

Figure 5 Throughput of all packets in presence of IPS for all attacks

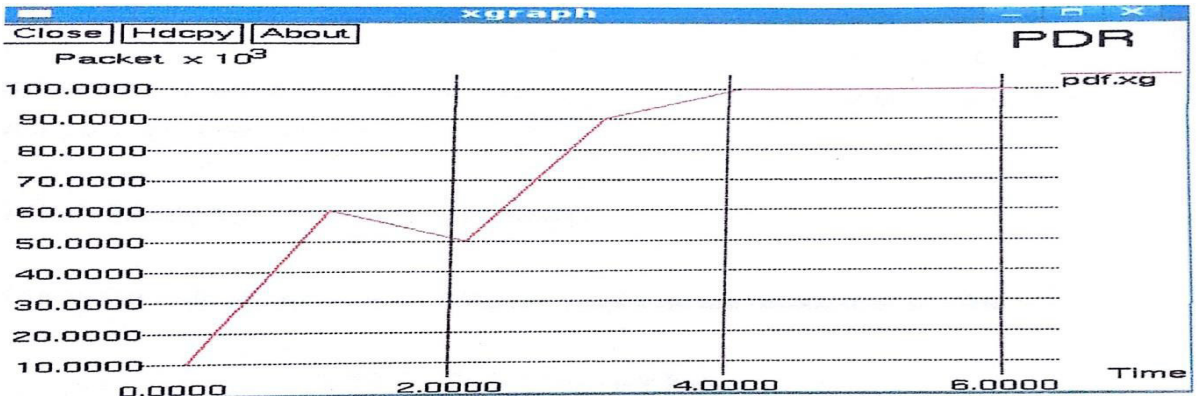

Figure 6 Packet delivered in time under all attacks with use of IPS

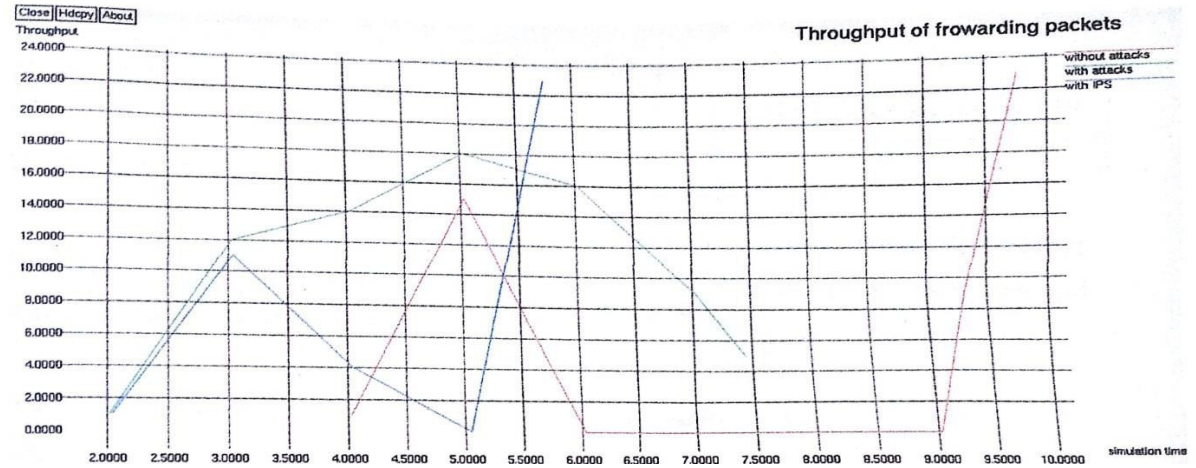

Figure 7 Throughput in all cases

Based on the results, we obtain the following results which clearly shown in table 3. The packet delivery ratio is remaining same in both without attacks and with attacks under IPS. The packet drop is zero by using intrusion mechanism system even though attacks are present.

PARAMETERS	WITHOUT ATTACKS	WITH ATTACKS	WITH ATTACK UNDER IPS
Packet delivery ratio	1.000	0.606	1.000
Packet drop	0	24	0
Jitter	7.86	6.79	11.21

6 CONCLUSION

The proposed method not only identifies the attack, it also identifies the range and extension of attack. This proposed system provides the noble solution and identify the attack is clearer by using the fuzzy logic technique. The system also contains IPS mechanism technique which gets input from fuzzy technique and provides the secure data communication over the network. IPS also monitor for the traffic of black hole and gray hole attacks. The result clearly shown this method detects the attack in an efficient manner when compared to existing method. Future work includes the reduction of jitter value which is more in presence of IPS, which is because of route modification in presence of attacks.

REFERENCES

1. Akansha Saini and Harish Kumar "Effect of Black hole attack on AODV Routing Protocol in MANET", International Journal of Computer Technology, Vol 1, no 2, December 2010.
2. Ekta Kamboj, "Detection of black hole on AODV in MANET using fuzzy" Journal of current computer science and technology, vol.1, no 6, pp 316-318, 2011.
3. Ganapathy S, Yogesh P and Kannan A "Intelligent agent based intrusion detection system using enhanced multiclass SVM", Hindawi Publishing Corporation, Computational Intelligence and Neuroscience, 2012.
4. Hu Y, Perrig A and Johnson B, "A Secure on Demand Routing Protocol for Ad Hoc networks", Proceeding of MobiCom, pp. 23-28, September 2002.
5. Hu Y, Perrig Y and Johnson B, "Rushing attack and Defences in Wireless Ad Hoc Networks Routing Protocols", Proceeding of 2nd ACM workshop on Wireless Security, New York, 2003.
6. Jungwon Kim and Peter J. Bentley "The Artificial Immune System for Network Intrusion Detection: An Investigation of Clonal Selection with a Negative Selection Operator", 2001.
7. Kurosawa S and Jamalipour A, "Detecting Black hole Attack on AODV- based Mobile Ad Hoc Networks by Dynamic Learning Method", International Journal of Network Security , Vol.5, November 2007.
8. Nadeem A and Howarth M, "Adaptive intrusion detection & prevention of Denial of Service attacks in MANETs", Proceeding of ACM 5th International Wireless Communication and Mobile Computing Conference, Germany, June 2009.
9. Padilla E, Aschenbruck N, Martini P, Jahnke M and Tolle J, "Detecting Black Hole Attack in Tactical MANETs using Topology Graph", Proceeding of 32nd IEEE Conference on Local Computer Networks, 2007.
10. Pirrete M and Brooks M, "The Sleep Deprivation Attack in Sensor Networks: Analysis and Methods of Defence", International Journal of Distributed Sensor Networks, Vol.2, No.3, pp. 267-287, 2006.
11. Poonam Yadav, Rakesh Kumar Gill and Naveen Kumar, "A Fuzzy Based Approach To Detect Black Hole Attack", International Journal Of Soft Computing and Engineering, ISSN: 2231-2307, vol 2, no 3, July 2012.
12. Revathi B, Geetha D, „A Survey of Cooperative Black and Gray hole Attack in MANET", International Journal of Computer Science and Management Research, Vol 1, no 2, September 2012.
13. Shanshan Zheng, Tao Jian and John S: "Intrusion Detection of in-band wormholes in MANET using advanced statistical methods", IEEE 2008.
14. Srinivas Mukkamala, Guadalupe Janoski, Andrew Sung "Intrusion Detection Using Neural Networks and Support Vector Machines", Proceedings of IEEE International Joint Conference on Neural Networks, pp. 1702-1701, 2002.
15. Steve Hofmeyr at all, "Intrusion Detection Using Sequences of Systems Call", Journal Of Computer Security, vol 6, pp 151-180, 1998.
16. Susan Bridges and Rayford Vaughn, "Fuzzy Data Mining and Genetic Algorithms Applied To Intrusion Detection", Proceedings 23rd National Information Security Conference, pp 1-19, October 2000.
17. Van Der Vorst H A, "Computational Methods for Large Eigenvalue Problems", in Handbook of Numerical Analysis, vol. 8, pp. 3-179, 2002.
18. Vijayan R, Mareeswari V and Ramakrishna K "Energy based trust solution for detecting selfish nodes in MANET using fuzzy logic", International Journal of Research and review in computer science, vol.2 No.3, June 2011.
19. Wang Yu, "Using Fuzzy Expert System based on Genetic Algorithm for Intrusion Detection System", April 2009.
20. Xiaopeng G and Wei C, "A Novel Gray Hole Attack Detection Scheme for Mobile Ad Hoc Networks," Proceeding of IFIP International Conference on Network & Parallel Computing, 2007.
21. Yi P, Dai Z and Zhang S, "Resisting Flooding Attack in Ad Hoc Networks", Proceeding of IEEE Conference on Information Technology: Coding and Computing", Vol.2, pp. 657-662, 2005.