International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2017 IJSRCSEIT | Volume 2 | Issue 2 | ISSN : 2456-3307

Intrusion Detection System by Using Friends Algorithm

K. Thennarasu, V. Karuppuchamy
Department of Computer Science and Engineering, Muthayammal Engineering College,
Rasipuram, India

ABSTRACT

Mobile Ad hoc Networks (MANETs) have been highly vulnerable to attacks due to the dynamic nature of its network infrastructure. Among these attacks, routing attacks have received considerable attention since it could cause the most damages to MANET. Friend based Ad hoc routing using Challenges to Establish Security (FACES) is an algorithm to provide secure routing in ad hoc mobile networks. The network is able to effectively isolate the malicious nodes in the ad hoc network. The information about the malicious nodes is gathered effectively by using Challenges. The drawback is that, the nodes are divided into friend list and question mark list. The question mark list nodes are not sure legitimate nodes. In my project, we propose a risk-aware response mechanism to the identify routing attacks. Our risk-aware approach is based on an Extended Dempster's-Shafer mathematical theory of evidence introducing a notion of importance factors. Using Dempster's Shafer Theory we can fix that the nodes are present in the question mark list are malicious nodes.

Keywords : FACES, MANET, Dempster's Shafer Theory

I. INTRODUCTION

MANET's are used to setup wireless communication without a predefined infrastructure and centralized administration. The network topology of the MANET will be frequently changed due to its mobility. Each mobile node in the network plays a router role while transmitting data over the network, because there are no specified node for routing [10]. The transmission of mobile host is received by all hosts within the transmission range due to the broadcast nature of wireless communication and omni directional antennae. When two wireless hosts are not within the transmission range in Ad hoc networks, other mobile hosts located between them can forward their messages, which effectively build connected networks. MANETs spread in opposing and unfriendly environment, where central authority is not needed[10].

Intrusions in information systems are the activities that violate the security of the system. Intruder is any person misbehaves in the network or trying to compromise any node in the network [11]. Intrusion Detection System (IDS) is the process of identifying intruder in the network. When any intruder is present in the network, IDS provide alert information to all the nodes in the network. Once intruder is found, the response may be either automatic or manual. After the detection of intruder, IDS isolate the individual (malicious) node or the entire path. Intrusion Detection is the most complicated problem in MANET [15]. Intrusion Detection System can be split into three major categories based on the intrusion detection approaches such as, Anomaly Based Intrusion Detection (or) Behavior Based Intrusion Detection, Misuse detection (or) Knowledge Based Intrusion Detection System, Specification Based Intrusion Detection System [11].

Anomaly Based Intrusion Detection System (ABID) monitors the normal behavior of the network, compared to the current behavior of the network to detect the intrusion in the network. Anomaly Based Intrusion Detection System consists of two phases such as training and testing [11]. Knowledge Based Intrusion Detection System (KBID) monitors the normal behavior of the network. From that behavior, it maintains knowledge about the signatures or patterns of well-known attacks and searches if there is any match to detect the intruder in the network. It has knowledge about only the specific tasks, so it can find only known attacks [11]. Specification Based Intrusion Detection System (SBID) explicitly define specifications as a set of constraints. They use this specification to monitor the routing protocol operations to detect operations in the network [11]. In this approach it contains the usual behavior of the network, it tests the behavior of the nodes in the network with the specified behavior, if there is any deviation that particular node is considered as intruder and generate an alarm [11].

II. RELATED WORK

Marti.et.al [1] suggested this technique. This is used for identifying misbehaving nodes in the network. This misbehaving node causes many problems such as, overloaded, selfish and dropping packets in the network. The misbehavior node is identified by using watchdog and path rater techniques. The sender sends any packet to the neighbor, the watchdog monitors continuously, whether the next node forwards the packet or not. The path rater run by each node in the network, which combines the knowledge of malicious nodes with link reliability data to chose the most reliable route. The limitations are ambiguous collisions and temporary isolation. V. Frias et.al [8] suggested the BARTER mechanism. BARTER is a mechanism that automatically creates and updates admission and access control policies for MANETs based on behavior profile. It is an adaptation mechanism for fully distributed network. MANET members initially exchange their behavior profiles and compute individual local definitions of normal network behavior. The limitations are, require agreement among fixed amount of MANET to exchange the network status. Fixing the threshold. Instead of define the behavior, it can exchange behavior profiles. Sanjay et.al [9] suggested FACES algorithm. FACES is an algorithm, which is used to provide secure routing between the nodes. The source sends challenge to the neighbor node, when the neighbor node forwards the packet to the next node, it will be added into the friend list otherwise it will be added into the question mark list. The nodes are rated based on the number of transmissions done. It can’t provide information about the question mark list nodes are either legitimate or malicious nodes. This method effectively isolate the malicious nodes in the network. No need to continuously monitor the traffic in the network. The limitation is that, when any node is compromised, then the whole network is intruded. J. Joseph et.al [2] suggested CRADS technique. CRADS is the mechanism to discover the malicious nodes and different types of denial of service attacks by violating the information. This technique is used to improve the accuracy of the network. When there is no cross layer interaction then the routing can select between several routes and have no information about congestion or malicious nodes. It selects a congested route or it selects a route that includes malicious nodes. With the help of cross layer interaction, the routing forwards possible route choices to MAC and MAC decides the possible routes using congestion and IDS information as well as returns the result to the routing. This cross layer technique using IDS leads to increase the detection rate. The detection rate is based on the number of misbehaving nodes, the misbehaving nodes increase the true positives and reduce the false positives in MANET. The limitation is that, CRADS can easily detect the intruder, but the intrusion response is lack.

A. Nadeem et.al [3] suggested Generalized Intrusion Detection and Prevention(GIDP) technique. Generalized Intrusion Detection and Prevention (GIDP) is the combination of Anomaly Based Intrusion Detection (ABID) and Knowledge Based Intrusion Detection (KBID). This is not only used for secure the MANET and also it has capability to detect new types of intrusions in the network. ABID gets training from the previous traces. It is used to detect an intrusion in the network. KBID is used to identify the specific attack using the set of rules. GIDP monitors the network and collects audit data specific for intrusion detection throughout the network. The limitations are, performs hypothesis test for each variable, so it takes more time. Lack of intrusion response. H. Debar et.al [6] suggested neural network technique. A back propagation neural network called Neural Network Intrusion Detector (NNID) was trained in the identification task and tested on a system of 10 users. The NNID anomaly intrusion detection system is based on identifying a legitimate user based on the distribution of commands, the user executes. Measure the performance of the network, when the network suggestion is deviate from the actual user or if the network does not have a clear suggestion, provide alert. The limitations are, when the behavior changes frequently, the false positives are increased. Prone to generate false alarms. Training is needed to identify the user. T. Haniotakis et.al [4] suggested Disjoint Multipath Routing (DMR) technique. DMR provides secure routing for data transmission, between the nodes. Before data transmission we have to establish connection between the nodes. This is used to find the shortest path between the source and destination. Dijikstra's algorithm provides a set of paths between the two nodes, this is the solution for routing problem. From the set of paths higher priority path is chosen for transmission of data. The path is selected based on the priority. The priority is based on the number of the edges a node directly linked in the network. The limitations are priority is assigned based on the direct interactions with other nodes in the network. Trust is also based on the acknowledgements. Encrypted messages are sent separately, when one packet is missed, we can't get the original message.

P. Narula et.al [5] suggested Trusted Multipath Routing (TMR) technique.TMR provides security using trust based multipath routing. The non trusted nodes in the routes are avoided based on the trust level. The trust level is assigned between the range -1 and 4. Trust level assignment is based on the number of direct interactions with its neighbors. A trust level 4 represents complete trust and -1 represents a complete distrust. A node with a trust level of -1 is a certified malicious node. All the packets that are received from these nodes are dropped immediately. The limitations are, trust is assigned based on the direct interactions with other nodes in the network. Trust is also based on the acknowledgement. C.Piro et.al [7] suggested the Sybil attack detection techniques. Each node in a MANET requires a unique address to participate in routing, through which nodes are identified. In a MANET there is no central authority to verify these identities. This is an example of impersonation attack. There are two methods to identify Sybil attacks such as, Passive Ad hoc Sybil Identity Detection (PASID) and PASID with Group Detection (PASID-GD). In Passive Ad hoc Sybil Identity Detection (PASID), a single node can detect Sybil attacks by recording the identities, namely MAC or IP addresses of other nodes it hears transmitting. In this second method, PASID with *Group Detection (PASID-GD), is the extension of PASID. It reduces the false positives that can occur when a group of nodes moving together is falsely identified as a single Sybil attacker. The limitations are, an attacker can corrupt trust in legitimate nodes. False positives can also occur if a collection of nodes moves together in close proximity either accidentally or intentionally. Sybil attackers may actively avoid detection by changing identities frequently.

III. PROPOSED SYSTEM

In the proposed system, Extended Dempster's Shafer Theory is used to detect the malicious node in the network and based on the level of risk the node is either temporarily or permanently isolate from the network.

A. EXTENDED DEMPSTER - SHAFER THEORY OF EVIDENCE

The Dempster-Shafer mathematical theory of evidence is both a theory of evidence and a theory of probable reasoning. The degree of belief models the evidence, while Dempster's rule of combination is the procedure to aggregate and summarize a corpus of evidences. However, previous research efforts identify several limitations of the Dempster's rule of combination

1.Associative: For DRC, the order of the information in the aggregated evidences does not impact the result. A non associative combination rule is necessary for many cases.

2.Nonweighted: DRC implies that we trust all evidences equally. However, in reality, our trust on different evidences may differ. In other words, it means we should consider various factors for each evidence. Yager, Yamada and Kudo proposed rules to combine several evidences presented sequentially for the first limitation. Wu et al. suggested a weighted combination rule to handle the second limitation. However, the weight for different evidences in their proposed rule is ineffective and insufficient to differentiate and prioritize different evidences in terms of security and criticality. Our extended Dempster-Shafer theory with importance factors can overcome both of the aforementioned limitations.

B. IMPORTANCE FACTORS AND BELIEF FUNCTION

In D-S theory, propositions are represented as subsets of a given set. Suppose θ is a finite set of states, and let 2^{θ} denote the set of all subsets of θ. D-S theory calls θ, a frame of discernment. When a proposition corresponds to a subset of a frame of discernment, it implies that a particular frame discerns the proposition. First, we introduce a notion of importance factors.

Definition 1. Importance factor (IF) is a positive real number associated with the importance of evidence. IFs are derived from historical observations or expert experiences.

Definition 2. An evidence E is a 2-tuple (m, IF), where m describes the basic probability assignment [5]. Basic probability assignment function m is defined as follows:

$$m(\Phi) = 0 \tag{1}$$

$$\Sigma_{A\varepsilon\theta}\, m(A) = 1 \tag{2}$$

According to [5], a function Bel : 2^{θ}-> [0, 1] is a belief function over θ if it is given by (3) for some basic probability assignment m : 2^{θ}-> [0, 1]

$$Bel(A) = \Sigma_{B\,\text{€}A}\, m(B) \tag{3}$$

for all A ε 2^{θ} describes a measure of the total beliefs committed to the evidence A.

Suppose IF1 and IF2 are importance factors of two independent evidences named E1 and E2, respectively. The combination of these two evidences implies that our total belief to these two evidences is 1, but in the same time, our belief to either of these evidences is less than 1. This is straightforward since if our belief to one evidence is 1, it would mean our belief to the other is 0, which models a meaningless evidence. And we define the importance factors of the combination result equals to (IF+IF2) / 2.

Definition 3: Extended D-S evidence model with importance factors: Suppose E1 = (m1, IF1) and E2 = (m2,IF2) are two independent evidences. Then, the combination of E1 and E2 is (m1(xor)m2, (IF+IF2)/2), where (xor) is Dempster's rule of combination with importance factors.

C. DEMPSTER'S RULE OF COMBINATION WITH IMPORTANCE FACTORS

In this section, we propose a Dempster's rule of combination with importance factors. We prove our combination rule follows the properties defined in the previous section.

Theorem 1: Dempster's Rule of Combination with Importance Factors: Suppose Bel1 and Bel2 are belief functions over the same frame of discernment θ, with basic probability assignments m1 and m2. The importance factors of these evidences are IF1 and IF2. Then, the function ḿ: 2^{θ}-> [0, 1] defined by

$$\acute{m}(\Phi) = 0 \tag{4}$$

Our proposed DRCIF is non associative for multiple evidences. Therefore, for the case in which sequential information is not available for some instances, it is necessary to make the result of combination consistent with multiple evidences. Our combination algorithm supports this requirement and the complexity of our algorithm is O(n), where n is the number of evidences. It indicates that our extended Dempster-Shafer theory demands no extra computational cost compared to a naive fuzzy-based method. The algorithm for combination of multiple evidences
is constructed as follows:

Algorithm 1: MUL-EDS-CMB

```
INPUT: Evidence pool Ep
OUTPUT: One evidence
|Ep|= sizeof(Ep);
While |Ep| > 1 do
    Pick two evidences with the least IF in Ep,
      named E1 and E2;
    Combine these two evidences,
      E=(m1(xor) m2, (IF+IF2) / 2),
    Remove E1 and E2 from Ep;
    Add E to Ep;
end
return the evidence in Ep
```

D. RISK-AWARE RESPONSE MECHANISM

In this section, we articulate an adaptive risk-aware response mechanism based on quantitative risk estimation and risk tolerance. Instead of applying simple binary isolation of malicious nodes, our approach adopts an isolation mechanism in a temporal manner based on the risk value. We perform risk assessment with the extended D-S evidence theory for both attacks and corresponding countermeasures to make more accurate response decisions.

Our risk-aware response system is distributed, which means each node in this system makes its own response decisions based on the evidences and its own individual benefits. Therefore, some nodes in MANET may isolate the malicious node, but others may still keep in cooperation with due to high dependency relationships.

Our risk aware response mechanism is divided into the following four steps:

1. Evidence collection:. In this step, Intrusion Detection System (IDS) gives an attack alert with a confidence value, and then Routing Table Change Detector (RTCD) runs to figure out how many changes on routing table are caused by the attack.
2.Risk assessment: Alert confidence from IDS and the routing table changing information would be further considered as independent evidences for risk calculation and combined with the extended D-S theory. Risk of countermeasures is calculated as well during a risk assessment phase. Based on the risk of attacks and the risk of countermeasures, the entire
risk of an attack could be figured out.
3.Decision making: The adaptive decision module provides a flexible response decision-making mechanism, which takes risk estimation and risk tolerance into account. To adjust temporary isolation level, a user can set different thresholds to fulfill her goal.
4.Intrusion response: With the output from risk assessment and decision-making module, the corresponding response actions, including routing table recovery and node isolation, are carried out to mitigate attack damages in a distributed manner.

Dr. Walter A. Shewart, Let P be a sample statistic that measures the quality characteristic of interest, and the mean of P is μp and the standart deviation of P is σp. The center threshold (CT), the upper threshold (UT) and lower threshold (LT) equation is stated in:

$$\mathbf{UT = \mu p + k\sigma p} \qquad (5)$$

$$\mathbf{CT = \mu p} \qquad (6)$$

$$\mathbf{LT = \mu p - k\sigma p} \qquad (7)$$

Where k is the distance of the control limit from the center line. A common choice for k is 3. The k value is also used by [13] in their research in detecting the intrusion activity based on audit trail.

E. RISK ASSESSMENT

Since the attack response actions may cause more damages than attacks, the risks of both attack and response should be estimated. We classify the security states of MANET into two categories: {Secure,Insecure}. In other words, the frame of discernment would be {Φ, {Secure}, {Insecure}, {Secure,Insecure}}. Note that {Secure, Insecure} means the security state of MANET could be either secure or insecure, which describes the uncertainty of the security state. Bel{Insecure} is used to represent the risk of MANET.

F. RESPONSE TO ROUTING ATTACKS

Node isolation may be the most intuitive way to prevent further attacks from being launched by malicious nodes in MANET. To perform a node isolation response, the neighbors of the malicious node ignore the malicious node by neither forwarding packets through it nor accepting any packets from it. On the other hand, a binary node isolation response may result in negative impacts to the routing operations, even bringing more routing damages than the attack itself.

G. SELECTION OF EVIDENCES:

Our evidence selection approach considers subjective evidence from experts' knowledge and objective evidence from routing table modification. We propose a unified analysis approach for evaluating the risks of both attack (RiskA) and countermeasure (RiskC).

Evidence 1: Alert confidence: The confidence of attack detection by the IDS is provided to address the possibility of the attack occurrence. Since the false alarm is a serious problem for most IDSs, the confidence factor must be considered for the risk assessment of the attack. The basic
probability assignments of Evidence 1 are based on three equations given below:

Alert Confidence c = (No. of Packets Dropped +

No. of Packets Modified) / Total No.of
Packets Received (8)

m(Insecure)= c; c is confidence given by IDS (9)

m(Secure)= 1 - c (10)
m(Secure, Insecure)= 0 (11)

Evidence 2: Missing entry. This evidence indicates the proportion of missing entries in routing table. Link with holding attack or node isolation countermeasure can cause possible deletion of entries from routing table of the node.

Evidence 3: Changing entry I. This evidence represents the proportion of changing entries in the case of next hop being the malicious node. In this case, the malicious node builds a direct link to this node. So, it is highly possible for this node to be the attacker’s target. Malicious node could drop all the packages to or from the target node, or it can behave as a normal node and wait for future attack actions. Isolating a malicious node cannot trigger this case.

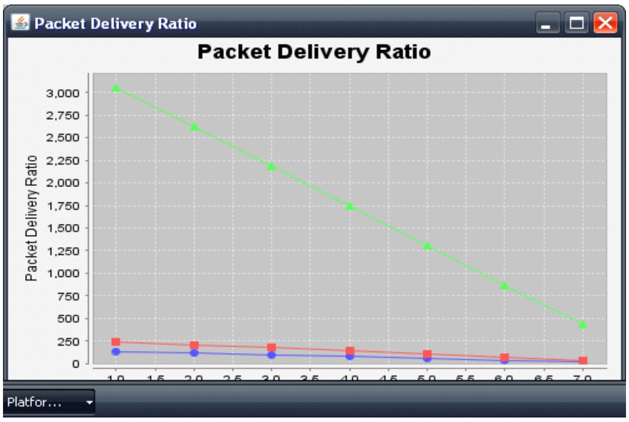
Evidence 4: Changing entry II. This evidence shows the proportion of changed entries in the case of different next hop (not the malicious node) and the same distance. We believe the impacts on the node communication should be very minimal in this case. Both attacks and countermeasures could cause this case.

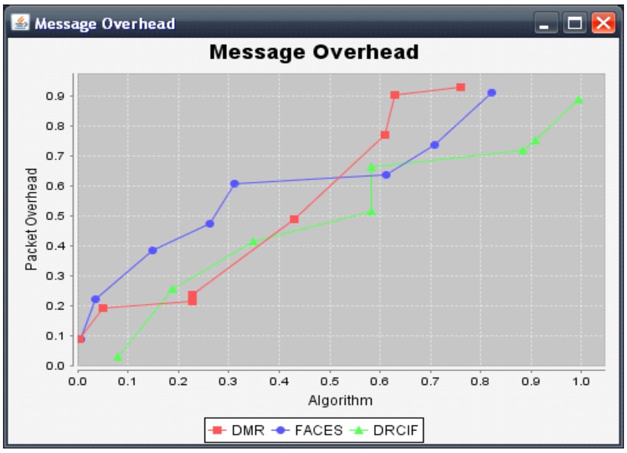
IV.PERFORMANCE EVALUATION

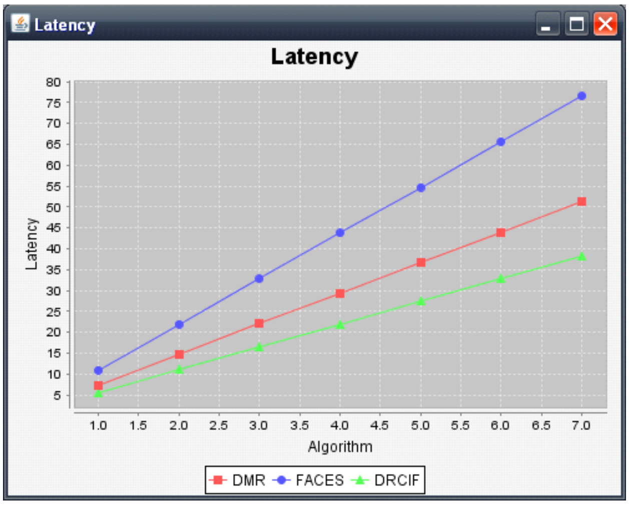
System performed with the network simulator (NS) 2.3.4 environment on a platform Linux. The system is running on a laptop with Core 2 Duo T7250 CPU and 3 GB RAM. In order to compare our result we assume scenario with 20 nodes using TCP protocol. Both the physical layer and MAC 802.11 are included in the wireless extension of NS2. We are using the following metrics:

- Packet Delivery Ratio
- Packet Overhead
- Mean latency

Packet Delivery Ratio: It is the ratio between the number of packets sent by the sources and the number of packets received by the destination (sink).
Packet Overhead: It is the number of transmitted routing packets. If a message sent through four hops it will be treated as four packets.
Mean Latency: It is the average delay between when the packets are transmitted from the source and when they received.







V. FUTURE WORK

Routing table recovery includes local routing table recovery and global routing recovery. Local routing recovery is performed by victim nodes that detect the attack and automatically recover its own routing table. Global routing recovery involves with sending recovered routing messages by victim nodes and updating their routing table based on corrected routing information in real time by other nodes in MANET. Routing table recovery is an indispensable response and should serve as the first response method after successful detection of attacks.

VI.CONCLUSION

Network environment with 'n' number of nodes are formed. By sample twenty number of nodes are taken. Our Extended Dempster's Shafer Theory will performs better than other protocols. Dempster's Shafer Theory fix that the Question mark list nodes are malicious nodes. Node activity will be analyzed by calculating the packet delivery ratio, packet overhead, mean overhead and mean latency.

VII. REFERENCES

[1]. S. Marti, T.J. Giuli, K.Lai and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks", Proc. International Conference on Mobile Computing and Networking, 2000, pp 255- 265.

[2]. J. Clerk J.Joseph, A.Das, B.Seet and B.Lee, "CRADS: Integrated Cross Layer approach for Detecting Routing Attacks in MANETs", Proc. IEEE Wireless Communication and Networking Conference (WCNC), 31st March -3rd April 2008.

[3]. A.Nadeem and M.Howarth, "A Generalized Intrusion Detection and Prevention Mechanism for Securing MANETs", Proc. IEEE International Conference on Ultra Modern Telecommunications and Workshops, St Petersburg Russia 2009.

[4]. T.Haniotakis, S. Tragoudas, and C. Kalapodas, "Security enhancement through multiple path transmission in ad hoc networks," in 2004 IEEE Int. Conf. Communications, Jun. 2004, vol. 7, pp. 4187–4191

[5]. P. Narula, S. K. Dhurandher, S. Misra, and I.Woungang, "Security in mobile ad-hoc networks using soft encryption and trust based multipath Network routing," Sci. Direct Comput. Commun., 2008, vol. 31, pp. 760–769.

[6]. H. Debar, M. Becker and D. Siboni, "A Neural Component for an Intrusion Detection System", Proc. IEEE Computer Society Symposium on Security and Privacy, Oakland, May 1992.

[7]. C.Piro, C.Shields and B.Levine, "Detecting the Sybil Attack in Mobile Ad hoc Networks", Proc. IEEE International Conference on Security and privacy in Communication Networks, Aug-Sep. 2006.

[8]. V. Frias-Martinez, S. J. Stolfo, and A. D. Keromytis, "BARTER:Behavior Profile exchange for behavior-based admission and access control in MANETs," presented at the Proc. 5th Int. Conf. Information Systems Security, Kolkata, India, 2009, pp. 193–207.

[9]. Sanjay K. Dhurandher, Mohammad S. Obaidat, Fellow, IEEE, Karan Verma, Pushkar Gupta, and Pravina Dhurandher, "FACES: Friend Based Ad Hoc Routing Using Challenges to Establish Security in MANETs Systems", IEEE systems journal, june 2011, vol. 5, no. 2.

[10]. Ziming Zhao, Hongxin Hu, Gail-Joon Ahn, and Ruoyu Wu,"Risk Aware Mitigation for MANET Routing Attacks",IEEE transactions on dependable and secure computing, march/april 2012, vol. 9, no. 2.

[11]. Adnan Nadeem ,Michael P.Howarth, "A Survey of MANET Intrusion Detection & Prevention Approaches for Network Layer Attacks", IEEE communications surveys & tutorials, accepted for publication.

[12]. Sanoop Mallissery, Jeevan Prabhu ,Raghavendra Ganiga, "Survey On Intrusion Detection Methods", "Proc. Of Int. Con/, on Advances in Recent Technologies in Communication and Computing 2011".

[13]. Ye, N & Chen,Q., "An Anomaly Based on Chi – Square statistic for International Journal of Quality and Reliability Engineering, Vol 17, pp. 105-112, 2001.