International Journal of Scientific Research in Computer Science, Engineering and Information Technology
© 2016 IJSRCSEIT | Volume 1 | Issue 1 | ISSN : 2456-3307

# Intrusion Detection and Secure Routing Techniques for Delay and Disorder Tolerant Monitoring Networks

**[1]Badde Hari Babu, [2]B. Srinivasa Rao, [3]Dr. S. Bhuvaneswari**

[1]Associate Professor CSE Department, Nova College of Engineering and Technology, Jafferguda, Hyderabad, Telangana, India
[2]Assistant Professor, CSE Department, Sri Rama Institute of Technology and Science, Kuppenakuntla, Khammam, Telangana , India
[3]Professor, CSE Department, Pondicherry University, Pondicherry, Tamil Nadu, India

## ABSTRACT

Intrusion detection is the act of detecting unwanted traffic on a network or a device. Monitoring of a node represent a serious threat against routing in delay tolerant network. Delay tolerant Network (DTN) became more popular in the research area recently, because of its application. The mechanism use for the DTN routing is the store-carry and forward approach. Main challenge for the DTN routing is that it discovers the route through the network without an end to end path so nodes in the network connect to the other nodes instantly. This article aim at to incorporate flow correlation information in to the classification process. Compared to contemporary approaches, IDNB (Intrusion Detection using Naive Bayes) demonstrates higher malicious behaviour detection rates in certain circumstances while does not greatly affect the network performances. NB is one of the earliest classification methods applied in intrusion detection system which is an effective probabilistic classifier employing the Bayes' theorem with naive feature independence assumptions. This paper also review about DTN, types of routing techniques and its issues, some popular routing protocols and their performance in terms of Delay, message Delivery rate, Overhead, Controlling the number of replications of the node. TA could punish compensate the node based on its behaviors. Each node must pay deposit amount before it joins the networks, and the deposit will be paid after then node leave if there is no misbehaviors activity of node. In this paper also focus on security between the nodes in DTN. We introduced a secret key is generated, which is used to share the data. The secret key is automatically changed when the node joins a network and leaves a network based on fast randomized algorithm. So we can increase the level of security in delay tolerant network.

**Keywords :** IDS, IPS, DIDS, NIDS, OSI, Trusted Authority, Secret Key, DTN, Misbehavior.

## I. INTRODUCTION

Intrusion detection is the act of detecting unwanted traffic on a network or a device. An IDS can be a piece of installed software or a physical appliance that monitors network traffic in order to detect unwanted activity and events such as illegal and malicious traffic, traffic that violates security policy, and traffic that violates acceptable use policies.

In delay, tolerant network Communication is possible even if end-to-end connectivity is never achievable. DTN Exploiting node's mobility and using store-carry-forward fashion. this is a new type of network are different from other kinds of networks. Delay Tolerant Network (DTN) is a set of emerging networks that has extremely distinctive characteristics from the other wireless network and internet. E.g. The intermittent connectivity, Large Delays, Low error rates [1] Mostly Large Delay and frequent partitions are there so may be up- to-date information for the stable network is not available so Data transmission is the main issue for the DTN. This is caused by the high mobility and the density of the nodes is very low. This kind of characteristics make the routing difficult in the DTN[1] exist solutions do not work in the environment like

DTN networks because assumption is taken for the network is stable and the link failures are infrequent between the nodes. Therefore efficient routing is the still research area in DTN [1].Delay/ Disruption tolerant networks (DTN) also called as intermittently connected mobile networks (ICMN), are wireless networks where the high mobility and low density of the nodes in the network at any given time instance, the probability that there is an end-to-end path from a source to a destination is low[1][2] Delay (or disruption) tolerant networking, provides an alternative approach for a various wireless environments that challenge the limitations of the transport and routing layers in the TCP/IP model. TCP/IP based Internet routing [3] where end-to-end path exists between peers, end-to-end packet drop problem is small and Low delay path between source to destination. DTN routing usually follows store-carry-and-forward; i.e., after receiving some packets, a node stores and carries them around until it contacts another node and then forwards the packets. Since DTN routing relies on mobile nodes to forward packets for each other, the routing performance (e.g., the number of packets delivered to their destinations) depends on whether the nodes meet each other or not. Delay- tolerant networking (DTN) is an approach to computer network architecture that seeks to address the technical issues in heterogeneous networks that may lack continuous network connectivity. Disruption may exist because of the limits of wireless radio range, lack of mobile nodes, energy sources, attack, and noise. Delay tolerant network are those operating in mobile or extreme terrestrial domains, or planned networks in space. Delay tolerant network providing a convenient mode of communication for civilian and business purposes, DTNs networks are highly desirable for use in battle zones, relief efforts in remote area, and difficulty situations in disaster areas. In such cases, where no network infrastructures exist, DTNs network can provide a crucial mode of communication. Delay and disruption- tolerant networks (DTNs) are characterized by their lack of connectivity, resulting in a insufficiency of spontaneous end-to-end paths. A network of local networks supporting interoperability among them. An overlay on top of regional networks including the Internet accommodate long delays between and within regional networks and translate between regional network communication characteristics. The problems of DTNs can be affected by store-and-forward massage switching DTN routers need persistent storage for their queues because a communication link may not be available for a long time One node may send or receive data much faster or more reliably than the other node A message once transmitted may need to be retransmitted for some reasons. Assume communicating devices (nodes) in motion and or operation with limited power. When nodes must conserve power, or preserve secrecy links are shut down -> intermittent connectivity network partition. On the Internet, infrequent connectivity causes loss of data while DTNs disconnect delay with a store-and-forward approach. Network nodes may need to broadcast or connect during opportunistic contacts in which a sender and receiver make contact at an unscheduled time. The bundle layer a new protocol layer overlaid on top of heterogeneous region-specific lower layers with which application programs can communicate across multiple regions. Mainly nodes in DTNs are of two types which are more different from other networks.

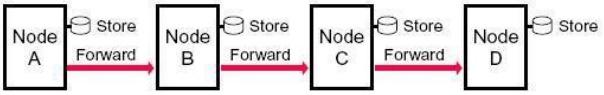



**Figure 1.** A node store and forward in DTNs

Selfish nodes minimize their contributions to the network community and maximize their own gains by placing conniving nodes into the network community (to grab information). Malicious nodes attack proper network operations and do not consider their own gains. DTNs security protocols have to be more invulnerable and powerful to handle these types of nodes. Also the characteristics of DTNs and characteristics of mobile ad-hoc networks are distant which makes these security protocols ineligible for DTNs. DTN-specific security solutions are required. Therefore, traditionally security system is not suitable. Messages in DTNs are called as bundles. They traverse through Delay Tolerant Network bundle agents who partake in bundle communications to form the DTN store-and-forward overlay network. Misbehave mean that to behave badly or improperly. In the adhoc network that totally depend upon the each other node for exchange of information. Misbehave in network that node not perform its task in a proper way. In computer networks an attack is any attempt to destroy, expose, alter, disable, steal or gain unauthorized access to or make unauthorized use of an asset. in this paper mainly focus on gray hole attack,

blackhole attack and wormhole attack. These attacks are harmful attack against the DTN network. Gray hole is a node that can transformation from behaving correctly to behaving like a black hole and it is literally an attacker and it will act as a normal node. Black holes are an attack in the network where incoming or outgoing traffic is silently discarded (or "dropped") without informing the source that the data did not reach its intended recipient. Worm hole attacks are a network that mine information to another network, that is it get the data from one network replicate it into another network through tunnel. DTNs network are suffer from lack of contemporaneous, end-to-end path High variation in network conditions, Difficulty to predict mobility, patterns Long feedback delay. Recently, there are quite a few proposals for misbehaviors detection in DTN, most of which are based on forwarding history verification (e.g., multi-layered credit, three-hop feedback transmission, or encounter ticket), which are costly in term of transmission overhead and verification cost. The basic idea of TA is to judge the node behavior based on the collected routing evidence. Before joining or leaving the node the contact to TA about the path before sending the packet one another node.

**1.1 Types of Ids's**

**Network-Based:**

A Network Intrusion Detection System (NIDS) is one common type of IDS that analyzes network traffic at all layers of the Open Systems Interconnection (OSI) model and makes decisions about the purpose of the traffic, analyzing for suspicious activity. Most NIDSs are easy to deploy on a network and can often view traffic from many systems at once. A term becoming more widely used by vendors is "Wireless Intrusion Prevention System" (WIPS) to describe a network device that monitors and analyzes the wireless radio spectrum in a network for intrusions and performs countermeasures which monitors network traffic for particular network segments or devices and analyzes the network and application protocol activity to identify suspicious activity. It can identify many different types of events of interest. It is most commonly deployed at a boundary between networks, such as in proximity to border firewalls or routers, virtual private network (VPN) servers, remote access servers, and wireless networks. The NIDS are also called passive IDS since this kind of systems inform the administrator system that an attack has or had taken place, and it takes the adequate measures to assure the security of the system. The aim is to inform about an intrusion in order to look for the IDS capable to react in the post.

**The Host Intrusion Detection System:**

Host-based intrusion detection systems (HIDS) analyze Network traffic and system-specific settings such as software calls, local security policy, local log audits, and more. A HIDS must be installed on each machine and requires configuration specific to that operating system and software. Host-Based, which monitors the characteristics of a single host and the events occurring within that host for suspicious activity. Examples of the types of characteristics a host-based IDPS might monitor are network traffic (only for that host), system logs, running processes, application activity, file access and modification, and system and application configuration changes. Host-based IDPSs are most commonly deployed on critical hosts such as publicly accessible servers and servers containing sensitive information.

**1.2 Classification of Routing Protocols**

The existing routing protocols in DTNs are classified with respect to their strategies for controlling message copies and forwarding decision of message to the destination [5] Number of destination: According to the number of destinations nodes to forward messages and routing can be classified into the three categories: 1) Unicast Routing: Only one destination for each message. 2) Multicast Routing: Destinations node could be one or group of destination nodes for each message 3) Broadcast Routing: All the nodes are the destination for the each message.

Number of copy: Depending on the number of copies utilized in the routing process the routing protocol can be classified into the two categories:

1) Single-copy routing protocols: Only a single copy for each message exists in the network at any time. 2) Multiple-copy routing protocols: Multiple copies of same message can be generated and distributed into the network. Moreover, multiple copy routing protocols can be further divided into flooding-based and quota based. a) Flooding-

based routing protocol: Dissemination or broadcast a copy of each message to as many nodes as possible. b) Quota-based routing protocol: It limits the number of message copies to flood in the network.

2) Available Network knowledge: Whether the forwarding decision is based on the knowledge derived from the nodes' encounters or not or from their history, protocols can as well be classified into two categories: 1) Deterministic routing protocol: Complete knowledge of node history encounter probability of nodes and node meeting times and period to make the forwarding decision 2) Non-deterministic routing protocols: Zero knowledge of pre- determined path between source and destination. These algorithms either forward the messages randomly or prediction based.

## II. RELATED WORK

A Delay Tolerant Network can be considered as an enhancement of the existing regional networks. This enhanced feature is called as the bundle layer. This layer is intended to function above the existing protocol layers and provide the function of a gateway when two nodes meet each other. The main advantage of this kind of protocol is flexibility. It can be easily linked with the already existing TCP/IP protocol networks or can be used to link two or more networks together [1-4]. The place of the bundle layer can be seen above the transport layer Bundles are the messages of nodes. By storing and forwarding entire bundles between nodes for the transfer of data from one node to another can be made reliable. The bundles contain source node ID and destination node ID, Time to Live-control information(TTL) and a bundle header. Whole bundles stores and transmit by the bundle layer between different nodes. The layers lower the bundle layers are selecting for their correctness to the communication environment of each filed. In DTNs at any given instant, there may not be any route to the next hop. In this case, the node must buffer the message in persistent storage, until a contact becomes available. Once the next hop stores the bundle in persistent storage, it is said to have taken custody of the bundle, and the node that have sent the message can delete its own copy of the bundle. Instead of waiting for the next hop to become available, the DTN gateways may themselves be mobile. Each node is associated with a persistent storage device like hard disk, where it can store the messages. In adhoc network have regular connectivity between their node. in DTNs follow the store-carry forward mechanism and store the packet in node buffer until any visible in transmission range. [1] proposed a social selfishness aware routing algorithm to allow user selfishness and provide better routing performance in efficient way. this approach deal with selfish node and also malicious node that not maximize their own benefit but to launch several attacks. [2] a secure multilayer credit-based incentive one of the most promising ways to address the selfishness issue and stimulate cooperation among selfish node in DTNs is using incentive scheme, which basically fall into two categories, reputation and credit- based scheme. Reputation based scheme rely on individual nodes to monitor neigh boring node traffic and keep track of each other. Where credit-based schemes introduce some form of virtual currency to regulate the packet forwarding relationships among different nodes. Our main focus on the detect the and avoid the packet loss during transmission from one node to other node and also provide security between the DTNs node. DTNs do not have the reliable link connection used in existing solution for node attacks.

## III. PERLIMINARY AND ROUTING ISSUES

Network Construction

In this network construction, first we have to construct a network which consists of ' n' number of Nodes. So that nodes can request data from other nodes in the network. Since the Nodes have the mobility property, they can move across the network. All nodes are registered in the network and each node pay some amount during the registration process. Network is used to store all the Nodes information like Node ID and other information. Also network will monitor all the Nodes Communication for security purpose.

Trusted Model

There are mainly two types of node are found in the network. Misbehaving node and normal node. a misbehaving node are two types firstly, selfish node that enjoy the service provide by network that refuse to carry packet for other node and malicious node that drop the received packet even if it has available buffer.

But it does not drop its own packet. A normal node may drop packet when its buffer overflow, but it follows our rule. Each packet has a certain life time and then expired packet should be lost no matter there is space or not. Such dropping can be easily identified if the expiration time of packet signed by the source. Trusted authority can be distinguished between the misbehaving and normal node based on its forwarding history from upstream and downstream.

Request Response based on trusted Authority

In this module, source node in network send data to destination means, before it sends the packet to trusted authority. That packet includes source node id, intermediate node id, destination node id, packet size and time. After receiving that packet trusted authority (TA) finds which node act as intermediate node. Then it sends request to all nodes for identifying intermediate node information. Based on that request each node sends the response to TA. Although TA auditing that information for identifying intermediate node trust worthiness using basic misbehavior detection algorithm.

Data Transmission

In this module, based on TA verification each node identifies the intermediate node behavior. Then source node securely transmits the data to destination node via honest intermediate nodes. Suppose node moves one network to another network means, network verifies if the node is honest or malicious based on probabilistic misbehavior detection algorithm. Then it refunds the amount based on node gentility. If the movable node is malicious means, network didn't refund the amount.

Node Construction based on Secret Key Assignment

In this module, network act as the main resource for all node. For the node registration process, network assigns secret key for each node in network based on fast randomized algorithm. All node information stored in the network. Also the network will maintain node location information. Suppose attackers will entire in network mean based on secret key it easily identifies the attacker. Network verifies node secret key for security purpose.

Key Changing based on Node Movement

In this module, source node wants to move one network means, its private key also changed by network based on fast randomized algorithm. Same time once node move to another network means, existing network completely change each node private key for security purpose. Suppose this source node hacks its previous network data means, it user their previous private key. But this private key. but this private key changed so it did not access previous network data.

Design Requirement Distributed

We require that a network rule liable for the administration of the network is only periodically available and consequently ineffective of controlling the operation minutiae of the network.

## IV. PROPOSED SCHEME

Introducing a secret key and a fast- randomized algorithm. We know that a DTNs network have unique feature of intermittent connectivity, which makes routing distant from other kind of wireless networks. Since an end to end connection is hard to arrangement, store-carry and forward is used to transfer the packet to the destination.

Proposed scheme is able to incorporate flow correlation information in to the classification process. IDNB (Intrusion Detection using Naive Bayes) demonstrates higher malicious behaviour detection rates in certain circumstances while does not greatly affect the network performances. NB is one of the earliest classification methods applied in intrusion detection system which is an effective probabilistic classifier employing the Bayes' theorem with naive feature independence assumptions. NB classifier is that it only requires a small amount of training data to estimate the parameters of a classification model.

Advantages

- Improved security.
- Less time consumption.
- No loss of data packet.
- Improved efficiency.
- Reduce the detection overhead adequately.
- Will reduce transportation overhead incurred by misbehavior detection and detect the malicious nodes effectively.
- Provide security against hackers, malicious software, Denial of services.

- NB with feature discretization demonstrates not only significantly higher accuracy but also much faster classification speed.

Secret Key

Secret key cryptography has been in use for thousands of years in a change of forms. Modern implementations normally take the form of algorithms which are completed by computer arrangement in hardware, firmware or software. The most of secret key algorithms are based on operations which can be performed very efficiently by digital computing systems.

Traditionally, this technique employs algorithms in which the key that is used to encrypt the original plaintext message can be calculated from the key that is used to decrypt the cipher text message and inversely. It has been used primarily to provide confidentiality. In secret key cryptography (also called symmetric key cryptography), only single key is used to perform both the encryption and decryption functions. The encrypted message can be freely sent from one location to another through an insecure intermediate, such as the Internet or a dial link. As the name signified, secret key cryptography relies on both parties keeping the key secret. If this key is negotiated, the security offered by the encryption process is eliminated.

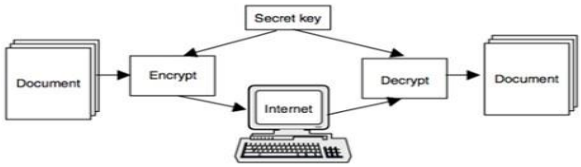



**Figure 2.** Secret Key

Secret key cryptography has powerful limitations that can make it impractical as a stand-alone solution for securing electronic transactions, especially among large communities of users that may have no pre-established relationships. The most important limitation is that some means must be devised to securely distribute and key management manage the keys that are at the heart of the system.

Transmitting Over an Insecure Channel

It is generally impossible to avoid eavesdropping when transmitting information. For instance, a telephone conversation can be tapped, a letter can be interrupted, and a message transmitted on a LAN can be received by unauthorized stations. If you and I agree on a shared secret key then by using secret key cryptography we can send messages to one another on a medium that can be tapped, without worrying about hearers. All we need to do is for the sender to encrypt the messages and the receiver to decrypt them using the shared secret. An hearers will only see unintelligible data. This is the classic use of cryptography.

Secure Storage on Insecure Media

If I info I want to preserve but which I want to assure no one else can look at I have to be able to store the media where I am sure no one can get it. Between expert thieves and court orders, there are very few places that are secure, and none of these is hard. If I invent a key and encrypt the info using the key, I can store it any location and it is safe so long as I can remember the key. Of course, forgetting the key makes the data fully lost, so this must be used with great care.

Authentication

The term strong verification means that someone can prove knowledge of a secret without revealing it. Strong authentication is possible with cryptography. Strong authentication is particularly effective when two computers are trying to communicate over an insecure network.

A Fast-Randomized Algorithm

This is an algorithm which gives excellent results when detect and verify on both source location as well as destination location networks and is much faster typically thousands of times faster than localized algorithms. It randomly provides a key for each node in network It gives a new randomized algorithm for achieving consensus among asynchronous processes that communicate by monitoring for every node in the entire network based on node key. An algorithm that employs a degree of randomness as part of its logic. The algorithm consistently uses uniformly random bits as an auxiliary input to guide its behavior in the hope of obtaining good performance in the "average case" over all possible choices of random bits. Properly, the algorithm's performance will be a

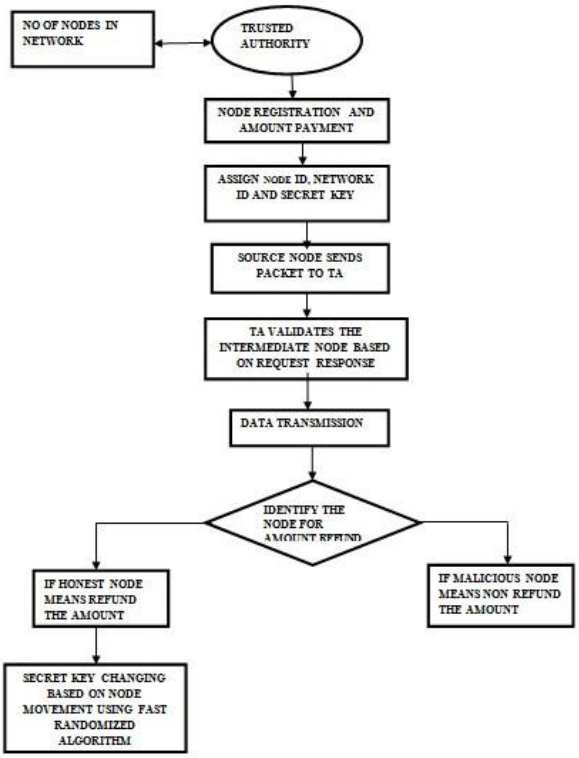
random variable determined by the random bits. thus either the executing time or the output (or both) are random variables. One has to analyze between algorithms that use the random input to reduce the expected running time or memory usage but always terminate with a correct result in a bounded amount of time and probabilistic algorithms. A fast- randomized algorithm is approximated using a pseudorandom number generator in place of a true source of random bits. Such a performance may deviate from the expected theoretical behavior. A fast- Randomized algorithm is particularly useful when faced with a malicious "adversary" or attacker who deliberately tries to feed a bad input to the algorithm.

Application of Algorithm

- It provides high security
- Easily identify the attacker
- Less time-consuming process
- Avoid packet loss
- Quick data transmission

Trusted Authority

TA which could launch the probabilistic detection for the target node and judge it by collecting the forwarding history evidence from its upstream and downstream nodes. Then, TA could punish or refund the node based on its behaviors. We assume that each node must pay a deposit amount before it joins the network and the deposit amount will be paid back after the node leaves if there is no misbehavior activity of the node. The basic misbehavior detection scheme to prevent malicious users from providing fake delegation/forwarding/ contact evidences. A should check the authenticity of each evidence by verifying the corresponding signatures which introduce a high transportation and signature verification overhead.




## V. CONCLUSION

In this paper, we mainly focus on the provide the security in the delay tolerant network node. So, we introduced secret key mechanism and also focus on avoid the packet loss during the transmission in the network. Secret key provide is a secure way to pass the information from one node to another node. It achieves better performance by the use of secret key. The secret keys are automatically generated. So, no one can guess the key of the node and it changing according to movement of node in the network. We also focus on the collection of exploits and attacks to classify and identify. We introduce a new technique called IDNB to detect the intrusion.

## VI. REFERENCES

[1]. Q. Li, S. Zhu, and G. Cao, "Routing in Socially Selfish Delay- Tolerant Networks," Proc. IEEE INFOCOM ‟10, 2010.

[2]. SMART: A Secure Multilayer Credit- Based Incentive Scheme for Delay-Tolerant Networks Haojin Zhu, Member, IEEE, Xiaodong Lin, Member, IEEE, Rongxing Lu, Student Member, IEEE, Yanfei Fan, and Xuemin (Sherman) Shen, Fellow, IEEE IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY , VOL. 58, NO. 8, OCTOBER 2009

[3]. H. Zhu, X. Lin, R. Lu, P.-H. Ho, and X. Shen, "SLAB: Secure Localized Authentication and Billing Scheme for Wireless Mesh Networks," IEEE Trans. Wireless Comm., vol. 17, no. 10, pp. 3858-3868, Oct. 2008.

[4]. Q. Li and G. Cao, "Mitigating Routing Misbehavior in Disruption Tolerant Networks," IEEE Trans. Information Forensics and Security, vol. 7, no. 2, pp.664-675, Apr. 2012.

[5]. S. Marti, T.J. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. ACM MobiCom ‟00, 2000.

[6]. R. Lu, X. Lin, H. Zhu, and X. Shen, "Pi: A Practical Incentive Protocol for Delay Tolerant Networks," IEEE Trans. Wireless Comm., vol. 9, no. 4, pp. 1483-1493, Apr.2010.

[7]. F. Li, A. Srinivasan, and J. Wu, "Thwarting Blackhole Attacks in Disruption- Tolerant Networks Using Encounter Tickets," Proc. IEEE INFOCOM ‟09, 2009.

[8]. W. Gao and G. Cao, "User-Centric Data Dissemination in Disruption-Tolerant Networks," Proc. IEEE INFOCOM ‟11, 2011.

[9]. A. Keranen, J. Ott, and T. Karkkainen, "The ONE Simulator for DTN Protocol Evaluation," Proc. Second Int‟l Conf. Simulation Tools and Techniques (SIMUTools ‟09), 2009.

[10]. A Probabilistic Misbehavior Detection Scheme toward Efficient Trust Establishment in Delay-Tolerant Networks Haojin Zhu, Member, IEEE, Suguo Du, Zhaoyu Gao, Student Member, IEEE, Mianxiong Dong, Member, IEEE, and Zhenfu Cao, Senior Member, IEEE.

[11]. http://en.wikipedia.org/wiki/Randomized_ algorithm

[12]. http://en.wikipedia.org/wiki/Key_ (cryptog raphy)

[13]. Langin, C. L. A SOM+ Diagnostic System for Network Intrusion Detection. Ph.D. Dissertation, Southern Illinois University Carbondale (2011)

[14]. Amoroso, E.: Intrusion Detection: An Introduction to Internet Surveillance, Correlation, Trace Back, Traps, and Response. Intrusion.Net Books (1999)