An Emerging Anomaly Detection Technique to Diminish the Routing Misbehavior in Mobile Ad hoc Network (MANET)

Chinmaya Kumar Nayak[1], Banchhanidhi Dash[2], Manoranjan Pradhan[3]

[1]Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), BPUT, Bhubaneswar, Odisha, India

[2]Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), BPUT, Bhubaneswar, Odisha, India

[3]Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), BPUT, Bhubaneswar, Odisha, India

Abstract: ***Mobile ad hoc network does not have traffic concentration points such as gateway or access points which perform behavior monitoring of individual nodes. Therefore, maintaining the network function for normal nodes when other nodes do not route and forward correctly is a big challenge. This paper, address the behavior based anomaly detection technique inspired by the biological immune system to enhance the performance of MANET to operate despite the presence of misbehaving nodes. Due to its reliance on overhearing, the existing watchdog technique may fail to detect misbehavior or raise false alarms in the presence of ambiguous collisions, receiver collisions, and limited transmission power. In this present scheme uses intelligent machine learning techniques that learns and detects each node by false alarm and negative selection approach.***

Keywords: Intrusion detection, anomaly detection, mobile ad hoc network, security.

1. Introduction

A Mobile Ad Hoc Network (MANET) is a collection of mobile nodes (hosts) which communicate with each other via wireless links either directly or relying on other nodes as routers. The network topology of a MANET may change rapidly and unpredictably. In a MANET, different mobile nodes with different goals share their resources in order to ensure global connectivity. However, some resources are consumed quickly as the nodes participate in the network functions. For instance, battery power is considered to be most important in a mobile environment. An individual mobile node may attempt to benefit from other nodes, but refuse to share its own resources. Such nodes are called selfish or misbehaving nodes and their behavior is termed selfishness or misbehavior [2]. One of the major sources of energy consumption in the mobile nodes of MANETs is wireless transmission [3]. A selfish node may refuse to forward data packets for other nodes in order to conserve its own energy. In order to mitigate the adverse effects of routing misbehavior, the misbehaving nodes need to be detected so that these nodes can be avoided by all well-behaved nodes. In this paper, we focus on the following problem:

1.1 Misbehavior Detection and Diminish:

In MANETs, routing misbehavior can severely degrade the performance at the routing layer. Specifically, nodes may participate in the route discovery and maintenance processes but refuse to forward data packets. How do we detect such misbehavior? How can we make such detection processes more efficient (i.e., with less control overhead) and accurate (i.e., with low false alarm rate and missed detection rate)?

The existing two extensions to the Dynamic Source Routing Algorithm (DSR) [4] to mitigate the effects of routing misbehavior: the watchdog and the path rater. In this technique, Watchdog's weaknesses are that it might not detect a misbehaving node in the presence of 1) ambiguous collisions, 2) receiver collisions, 3) limited transmission power, 4) false misbehavior, 5) collusion, and 6) partial dropping.

In this paper the emphasis is on behavior based intrusion detection techniques which assume that an intrusion can be detected by observing deviations from the normal or expected behavior of the nodes. The intrusion detection systems compare this behavior model with activities of normal node. When the deviation is observed, an alarm is generated.

The implemented behavior based anomaly detection to the underlying DSR, AODV and DSDV Source routing algorithms. The basic idea of the behavior-based approach involves Negative Selection Algorithm (NSA).The detectors are capable of distinguishing well-behaving nodes from the misbehaving nodes with a good degree of accuracy. The False positives (or False Alarms) could be minimized to good extent though some False Negatives exist because of subtle differences between good and bad behaviors in this experimentation.

Various approaches for router misbehavior detection and mitigation that have been proposed and studied in the literature. The details of Negative Selection Algorithm (NSA), and describes router misbehavior and attacking scenarios.

2. Related Work

The security problem and the misbehavior problem of wireless networks including MANETs have been studied by many researchers, e.g., [4], [5], [6], [7]. Various techniques have been proposed to prevent selfishness in MANETs. These schemes can be broadly classified into two categories: credit-based schemes and reputation-based schemes.

2.1 Credit-Based Schemes

The basic idea of credit-based schemes is to provide incentives for nodes to faithfully perform networking functions. In order to achieve this goal, virtual (electronic) currency or similar payment system may be set up. Nodes get paid for providing services to other nodes. When they request other nodes to help them for packet forwarding, they use the same payment system to pay for such services [8], [9], [10].The main problem with credit-based schemes is that they usually require some kind of tamper-resistant hardware and/or extra protection for the virtual currency or the payment system. I focus on reputation-based techniques in this paper instead.

2.2 Reputation-Based Schemes

The second category of techniques to combat node misbehavior in MANETs is reputation-based [11]. In such schemes, network nodes collectively detect and declare the misbehavior of auspicious node. Such a declaration is then propagated throughout the network so that the misbehaving node will be cut off from the rest of the network.

In [12], Marti et al. proposed a scheme that contains two major modules, termed watchdog and pathrater, to detect and mitigate, respectively, routing misbehavior in MANETs. Nodes operate in a promiscuous mode wherein the watchdog module overhears the medium to check whether the next-hop node faithfully forwards the packet. At the same time, it maintains a buffer of recently sent packets. A data packet is cleared from the buffer when the watchdog overhears the same packet being forwarded by the next-hop node over the medium. If a data packet remains in the buffer for too long, the watchdog module accuses the next hop neighbor of misbehaving. Thus, the watchdog enables misbehavior detection at the forwarding level as well as the link level. Based on the watchdog's accusations, the path rater module rates every path in its cache and subsequently chooses the path that best avoids misbehaving nodes. Due to its reliance on overhearing, however, the watchdog technique may fail to detect misbehavior or raise false alarms in the presence of ambiguous collisions, receiver collisions, and limited transmission power, as explained in [12].

The CONFIDANT protocol proposed by Buchegger and Le Boudec in [13] is another example of reputation-based schemes. The protocol is based on selective altruism and utilitarianism, thus making misbehavior unattractive. CONFIDANT consists of four important components—the Monitor, the Reputation System, the Path Manager, and the Trust Manager. They perform the vital functions of neighborhood watching, node rating, path rating, and sending and receiving alarm messages, respectively. Each node continuously monitors the behavior of its first-hop neighbors. If a suspicious event is detected, details of the event are passed to the Reputation System. Depending on how significant and how frequent the event is, the Reputation System modifies the rating of the suspected node. Once the rating of a node becomes intolerable, control is passed to the Path Manager, which accordingly controls the route cache. Warning messages are propagated to other nodes in the form of an Alarm message sent out by the Trust Manager. The Monitor component in the CONFIDANT scheme observes the next hop neighbor's behavior using the overhearing technique. This causes the scheme to suffer from the same problems as the watchdog scheme.

There exist some wireless intrusion detection systems WLAN IDS [14] that encompasses components such as data collection, intrusion detection and an additional secure database to log anomalies. Other IDS were designed to secure wireless networks (WLAN). One such IDS [15] suggest to detect intrusions such as abnormal routing table updates and attacks at the MAC layer.

3. Negative Selection Algorithm (NSA)

The Negative Selection Algorithm (NSA) is based on the principles of self/non-self discrimination in the immune system. It can be summarized as follows:

Define self as a collection S of elements in a feature space X, a collection that needs to be monitored. For instance, if X corresponds to the space of states of a system represented by a list of features, S can represent the subset of states that are considered as normal for the system. Generate a set F of detectors, each of which fails to match any string in S.

Monitor S for changes by continually matching the detectors in F against S. If any detector ever matches, then a change is known to have occurred, as the detectors are designed not to match any representative samples of S. In this work, I propose a hybrid approach for misbehavior detector generation

3.1 Anomaly detection

The anomaly detection process aims at distinguishing a new pattern as either part of self or non- self, given a model of the self (normal data) set. The problem space, denoted by X in an n - dimensional space; the self set is denoted as S and let N be the complementary space of S It is assumed that each attribute is normalized to [0, 1], then

Given the normal behavior of a system S the characteristic function of S defined

$$S \subseteq [0,1]^n \quad S \cup N = X, \quad S \cap N = \Phi$$

As NS (p) = 1, p £S

0, p £N is used to distinguish between self and non-self

In order to generate detectors through an evolutionary process, we used a structured genetic algorithm (sGA), which

is suitable for encoding different detector shapes [16].

3.2 The Structured GA

A structured GA (sGA) is a type of evolutionary algorithm [17] that incorporates redundant genetic material, which is controlled by a gene activation mechanism. It utilizes multi-layered genomic structures for its chromosome i.e. all genetic material (expressed or not) is 'structured' into a hierarchical chromosome. The activation mechanism enables and disables these encoded genes. The implicit redundancy has the advantages of maintaining genetic diversity necessary in solving complex search and optimization applications. The capacity to maintain such diversity however depends on the amount of redundancy incorporate in the structure.

The SGA as shown in Figure.1 interprets the chromosome as a hierarchical structure; thus, genes at any level can be either active or passive, and high-level genes activate or deactivate sets of low-level genes. Thereby, the dynamic behavior at any level, whether the genes will be expressed phenol typically or not, is governed by the high level genes.

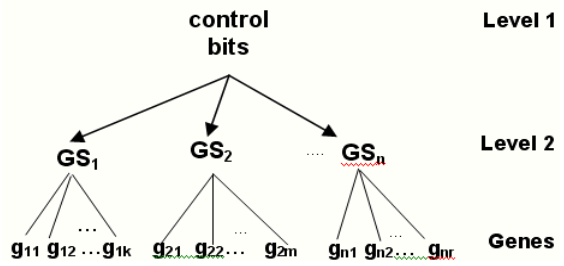
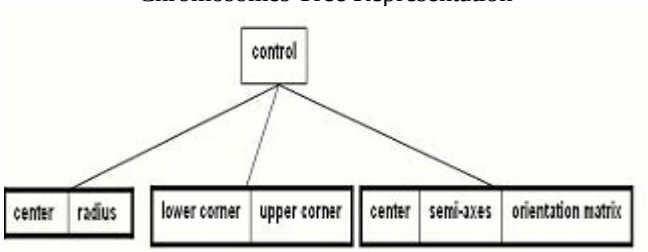


Figure 1: Structured GA representation of a chromosome with n different gene sets

This illustration shows that the representation scheme for a chromosome tree has a control gene activating one of the shapes in phenotype space where each shape identifies a detector shape. A detector is defined in an n- dimensional space as a geometrical shape, such as a hyper sphere, a hyper-rectangle or a hyper-ellipse. The matching rule is expressed by a membership function associated with the detector, which is a function of the detector sample pattern distance [18] (Euclidean or any other distance measure). A set of good samples (also known as self) represented by n-dimensional points are given as inputs to the algorithm.

Chromosomes Tree Representation



Chromosome Linear Representation

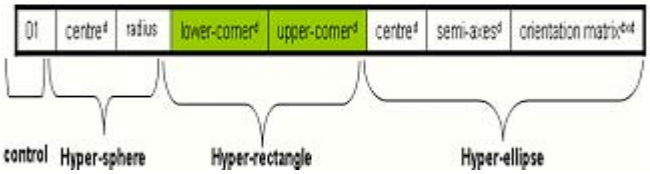


Figure 2: Encoding multi-shaped detectors: a chromosome having high level control and low level parameters for three different shapes: hyper spheres, hyper-rectangles and hyper-ellipses detectors.

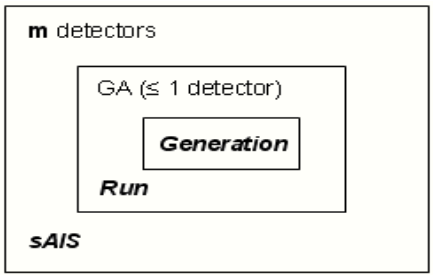


Figure 3: General framework for detector generation

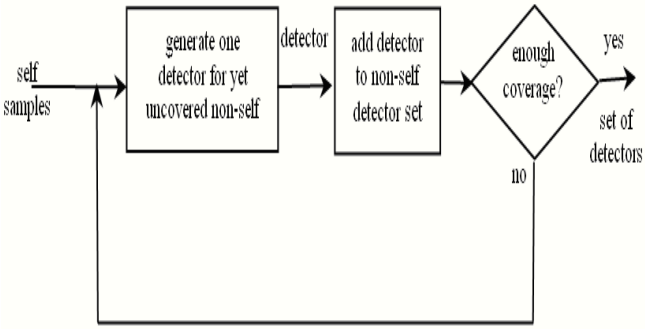


Figure 4: Modular subdivision of the detector generation process

As depicted in Figure 3, the goal of the algorithm is to evolve a set of detection rules to cover the non-self space. The iterative process to generate a set of detectors (Figure 4) is driven by two main goals: Minimize overlap with self, and Make the detectors as large as possible and keep them separate from each other, in order to maximize the non- self covering (This is referred to as the coverage parameter in all our experiments).In this work, we assumed that the self data points representing the events of good traffic network behavior while non-self data points represent the misbehaving event sequences.

4. Problem of Routing Misbehavior

In this section, we describe the problems caused by routing

misbehavior. Then, we illustrate detection of flooding attacks, and DoS attack scenarios.

4.1 Routing Misbehavior Model

The routing misbehavior model considered in this paper in the context of the DSR, AODV and DSDV protocol. Due to its popularity and recognized by IETF MANET group, we use these routing protocols to illustrate our proposed anomaly detection add-on scheme. The details of DSR, AODV and DSDV can be found in [5].

We focus on the following routing misbehavior: A selfish node does not perform the packet forwarding function for data packets unrelated to it. However, it operates normally in the Route Discovery and the Route Maintenance phases of the routing protocol. Since such misbehaving nodes participate in the Route Discovery phase, they may be included in the routes chosen to forward the data packets from the source. The misbehaving nodes, however, refuse to forward the data packets from the source. This leads to the source being confused. The existence of a misbehaving node on the route will cut off the data traffic flow. The source has no knowledge of this at all.

In this paper, we propose intelligent machine learning technique to detect such misbehaving nodes. Routes containing such nodes will be eliminated from consideration. The source node will be able to choose an appropriate route to send its data.

4.2 Detecting Router Misbehavior

Wireless Ad hoc networks using routing protocol such as DSR, AODV and DSDV are highly vulnerable to (packet) routing misbehavior due to misbehaving, faulty or compromised nodes. We describe detection of flooding attacks and two attack scenarios.

4.3 Detecting Flooding Attacks

From the work of [19] it was seen that 802.11b wireless networks suffers from some inherent flaws and are therefore prone to more attacks than wired networks because there is no need of any physical access to wireless networks. We first show how the above approach can be used to detect flooding attacks. We implemented two familiar attacks based on the guidelines in our previous work [19]. The two attacks are Denial of Service attack from an attacker machine outside the wireless network, and Denial of Service attack from a compromised machine inside the wireless network. The first attack was launched in a simulation environment consisting of some wireless stations and an Access Point (Figure 5), while the second one is implemented using a network simulator tool called Qualnet 4.5 (Figure 6). The detection results indicate that in all the three cases the Negative Detectors were able to detect the attacks with good detection rate. We briefly illustrate the attack scenario and the results for the Ad-hoc network case. The simulation scenario comprises of an Ad-hoc WLAN with three wireless stations communicating with each other (Figure 5), and established normal traffic flow. An attacker machine lunches a PING flood attack to a wireless node. This attack is launched by setting DoS attack in the configuration setting.

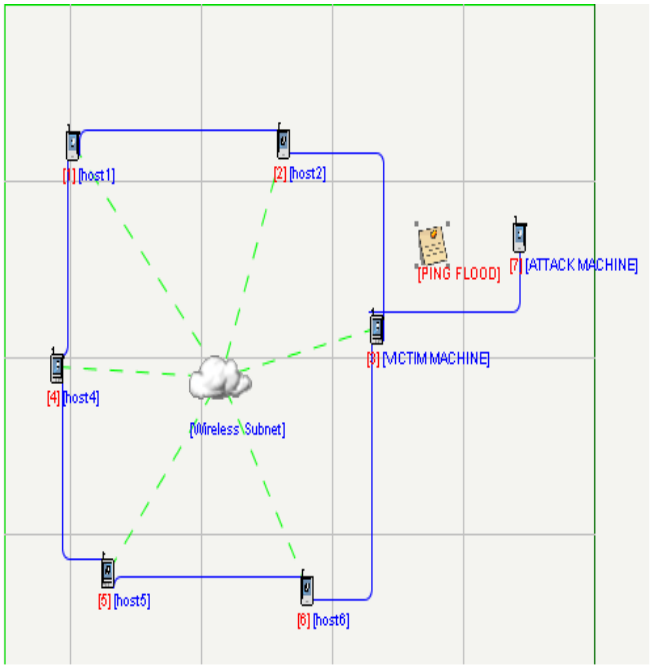


Figure 5: Ping Flood DoS in Ad-Hoc Network from an attacker machine

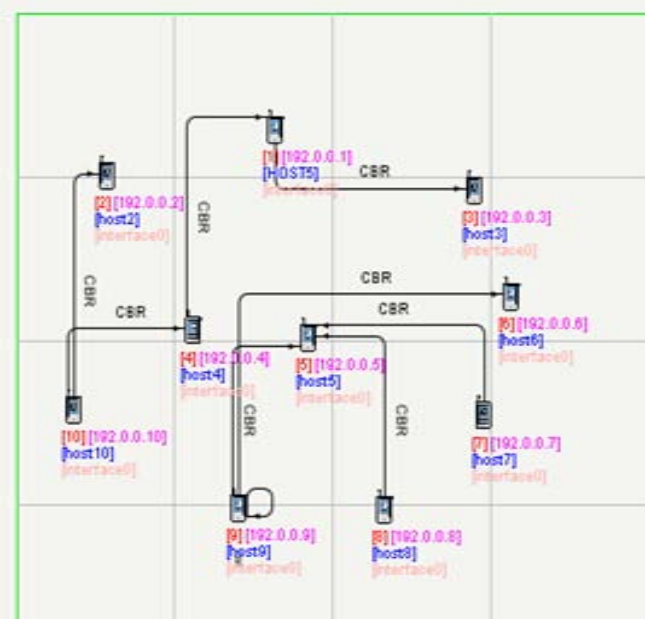


Figure 6: DoS attack by a compromised node in the Wireless network implemented

The ICMP (Internet Control Message Protocol) packet sequence numbers are collected at the Ad-hoc node different from the victim machine, which keeps pinging, on the victim machine throughout the experiments. The time taken for each packet to reach the destination node is noted when each ping (ICMP) packet is sent. It is observed that during the occurrence of an attack, there are some drops in the ICMP packets. In addition, the time taken to reach the destination host increased when the attack was launched.

Figure 6 shows a scenario with 10 nodes and the traffic flow among them. These nodes are labeled, ranging from Node 0 to Node 9. Constant Bit Rate (CBR) traffic is defined

between Node 0 and Node 2 Node 3 to Node 4, Node 4 to Node6, Node 5 to Node 3 Node 6 to Node 7, Node 1 to Node 8, Node 9 to Node 2, Node 8 to Node 7 and File Transfer Protocol (FTP) traffic flows between Node 1 and Node2. The start times for all these traffics are preset. The attack is launched from Node 0 to Node 2. The attack is simulated as DoS with heavy traffic flow in a short time interval. During these periods when the attack was launched, the number of legitimate packets received by the victim node (Node 2) was reduced. The sequence numbers resulting from the connection between different nodes and Node 2 were collected.

We are using this approach in order to test our detection approach, although a more realistic approach (the complete network profile rather than monitoring a single node) is used in this work for misbehavior detection [20], [21]. The primary objective was to evaluate our model in terms of good detection rates and low alarm rates for wireless ad-hoc network's routing layer

5. Conclusions

It is proposed to use behavior based anomaly detection learning technique in which learning of good behavior node and detection of misbehavior node is carried out in a ad-hoc wireless environment. The cooperative approach generated multi-shaped detectors (a set of rules) defining a boundary for the unknown regions of the behavior space. In certain cases, it would require a large amount of training (good) data as well as the number of efficient detectors [23],[24]. Sometimes, for very subtle misbehavior detection, more detectors with better coverage are necessary. Three set of protocol like DSR, AODV and DSDV, to test the effect of proposed approach. With the use of learning threshold for the detectors learning, certain subtle abnormalities are supposedly captured. It is more difficult to decide the behavior of a single node. This is mainly due to the fact that communication takes place between two nodes and is not the sole effort of a single node. Therefore, care must be taken before punishing any node associated with the misbehaving links. When a link misbehaves, either of the two nodes associated with the link may be misbehaving. In order to decide the behavior of a node and punish it, we may need to check the behavior of links around that node. This is a potential direction for my future work.

References

[1] C.Perkins and P.Bhagwat, "Highly dynamic destination-sequenced distance-vector routing (DSDV) for mobile computers," in proceedings of the ACM SIGCOMM'94 Conference on Communications Architectures, Protocol and Applications, London, UK, August 1994, pp.234-244.

[2] L. Buttyan and J.-P. Hubaux, "Security and Cooperation in Wireless Networks," http://secowinet.epfl.ch/, 2006.

[3] L.M. Feeney and M. Nilsson, "Investigating the Energy Consumption of a Wireless Network

[4] Interface in an Ad Hoc Networking Environment," Proc. IEEE INFOCOM, 2001.

[5] L. Zhou and Z.J. Haas, "Securing Ad Hoc Networks," IEEE Network Magazine, vol. 13, no. 6,

[6] Nov. /Dec. 1999.

[7] F. Stajano and R. Anderson, "The Resurrecting Duckling: Security Issues in Ad-Hoc Wireless Networks," Proc. Seventh Int'l Workshop Security Protocols, 1999.

[8] J. Kong, P. Zerfos, H. Luo, S. Lu, and L. Zhang, "Providing Robust and Ubiquitous Security

[9] Support for Mobile Ad-Hoc Networks," Proc. IEEE Int'l Conf. Network Protocols (ICNP '01), 2001.

I. Aad, J.-P. Hubaux, and E-W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. MobiCom, 2004.

[10] L. Buttyan and J.-P. Hubaux, "Enforcing Service Availability in Mobile Ad-Hoc WANs," Proc. MobiHoc, Aug. 2000.

[11] J.-P. Hubaux, T. Gross, J.-Y. LeBoudec, and M. Vetterli, "Toward Self-Organized Mobile Ad Hoc Networks: The Terminodes Project," IEEE Comm. Magazine, Jan. 2001.

[12] L. Buttyan and J.-P. Hubaux, "Stimulating Cooperation in Self-Organizing Mobile Ad Hoc Networks," ACM/Kluwer Mobile Networks and Applications, vol. 8, no. 5, 2003.

[13] S. Zhong, J. Chen, and Y.R. Yang, "Sprite: A Simple, Cheat-Proof,Credit-Based System for Mobile Ad-Hoc Networks," Proc. INFOCOM, Mar.-Apr. 2003.

[14] S. Marti, T. Giuli, K. Lai, and M. Baker, "Mitigating Routing Misbehavior in Mobile Ad Hoc Networks," Proc. MobiCom, Aug.2000.

[15] S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the CONFIDANT Protocol: Cooperation of Nodes, Fairness in Dynamic Ad-Hoc Networks," Proc. MobiHoc, June 2002.

[16] Y. Lim, T. Schmoyer, J. Levine and H. L. Owen. "Wireless Intrusion Detection and Response". In Proceedings of the 2003 IEEE workshop on Information Assurance United States Military Academy, NY: West Point.

[17] Y. Zhang and W. Lee. August 6-11, 2000. "Intrusion Detection in Wireless Ad-Hoc Networks". In Proceedings of the Sixth Annual International Conference on Mobile Computing and Networking, Boston: Massachusetts.

[18] S. Balachand ran, D. Dasgupta, F. Nino, D. Garrett, "Framework for Evolving Multi- Shaped Detectors in Negative Selection". Submitted to the IEEE Transactions on Evolutionary Computation, January 2006.

[19] D. Dasgupta and D. R McGregor, "sGA: A structured Genetic Algorithm". Research Report IKBS-11-93, April 1993.

[20] F. González, "A study of Artificial Immune Systems Applied to Anomaly Detection", .PhD. Dissertation, Advisor: Dr. Dipankar Dasgupta, The University of Memphis, May 2003.

[21] M. Kaniganti. "An Agent-Based Intrusion Detection System for Wireless LANs", Master's Thesis, Advisor: Dr. Dipankar Dasgupta. The University of Memphis, December 2003.

[22] S. Sarafijanovic and J.Y. Le Boudec. "An Artificial Immune System for Misbehavior Detection in Mobile Ad-Hoc Networks with Virtual Thymus, Clustering,

Danger Signal and Memory Detectors". In Proceedings of ICARIS-2004 (Third International Conference on Artificial Immune Systems), pp . 342-356, September 13-16, 2004, Catania, Italy

[23] J. Kim and P.J. Bentley. "The Artificial Immune Model for Network Intrusion Detection", 7th European Conference on Intelligent Techniques and Soft Computing (EUFIT'99), Aachen, Germany.

[24] Scalable Network Technologies, "Qualnet simulator-version 4.5," Software package 2008,[online]. Available : http://www.qualnet.com

[25] H. Miranda and L. Rodrigues, "Preventing Selfishness in Open Mobile Ad Hoc Networks," Proc. Seventh CaberNet Radicals Workshop, Oct. 2002.

[26] Meera Gandhi, S.K.Srivatsa," Detecting and preventing attacks using network intrusion detection systems", in the International Journal of Computer Science and Security, Volume: 2, Issue: 1, Pages: 49-58.

[27] N. Bhalaji, A.vShanmugam, Druhin Mukherjee, Nabamalika Banerjee." Direct trust estimated on demand protocol for secured routing in mobile Adhoc networks", in the International Journal of Computer Science and Security, Volume: 2, Issue: 5, Pages: 6-12.

Author Profile

Chinmaya Kumar Nayak is an Assistant Professor in the Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India. He is an author of the book "Data Structure Using C". He published many papers in national seminars and international journals. His research area includes image processing, adhoc networks etc.

Banchhanidhi Dash is an Assistant Professor in the Department of Computer Science& Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha ,India.

Manoranjan Pradhan holds a Ph. D Degree in Computer Science. He is presently working as a professor and Head of the Department of Computer Science & Engineering, Gandhi Institute for Technological Advancement (GITA), Bhubaneswar, Odisha, India. He has 14 years of teaching experience. He has published many papers in national and international journals. His research interests include Computer Security, Intrusion Detection and Soft Computing.