Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 11, November 2014, pg.212 – 222

RESEARCH ARTICLE

DETECTING MALICIOUS ATTACKS USING DYNAMIC THRESHOLD OPTIMIZATION ALGORITHM

R. Mehala*, S.Sathya, M.Sc., M.Phil.**
*M.Phil(Computer Science), Research Scholar,
Vivekanandha College for Women, Unjanai, Tiruchengode, India
******Assistant Professor in Computer Science
Vivekanandha College for Women, Unjanai, Tiruchengode, India

***Abstract:** The presence of malevolent nodes, this requirement may lead to serious security concerns; for instance, such nodes may disrupt the routing process. So that there is no guarantee for our information has been sent securely. In this thesis to investigate the feasibility of adjusting our CBDS approach to address other types of collaborative attacks on MANETs and to investigate the integration of the CBDS with other well-known message security schemes in order to construct a comprehensive secure routing framework to protect MANETs against miscreants. The proposed scheme use dynamic threshold optimization algorithm to solve other type of attacks such as wormhole attacks, Sybil attacks, routing attacks. By using this algorithm it wills automatically self configure itself to check the threshold value low or high before the data is sent. If the threshold value is high, no attacks are in the node. If the threshold value is low means some malicious nodes are in MANET. The attacked nodes are removed and choose alternative path to send data to destination. Through sensing the network to find possible node in the network to send our information in a secured manner.*

***Keywords:** Mobile Computing, MANET, DTO Method, GRA Method*

1. INTRODUCTION

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage. Mobile computing offers significant benefits for organizations that choose to integrate the technology into their fixed organizational information system.

Mobile computing is made possible by portable computer hardware, software, and communications systems that interact with a non-mobile organizational information system while away from the normal, fixed workplace. Mobile computing is a versatile and potentially strategic technology that improves information quality and accessibility, increases operational efficiency, and enhances management effectiveness.

Mobile Ad-hoc networks (MANET) are self configuring and self-organizing multi hop wireless networks where, the network structure changes dynamically. In a MANET nodes (hosts) communicate with each other via wireless links either directly or relying on other nodes as routers. The nodes in the network not only acts as hosts but also as routers that route data to/from other nodes in network The operation of MANETs does not depend on preexisting infrastructure or base stations. Network nodes in MANETs can move freely and randomly.

ROUTING ATTACKS IN MANETS

Routing plays a very important role in MANETS. It can also be easily misused, leading to various types of attack in the network. Routing protocols in general are more easily attacked by malicious nodes. These protocols are usually not designed with security function and often they are very vulnerable to node misbehavior attacks. It is true for MANET routing protocols because they are designed for minimizing the level of overhead and for allowing every node to participate in the routing process.

Various routing attacks caused by attackers in MANET are:

Black Hole Attack

In this attack a malicious node makes use of routing protocols to misrepresents that it having the shortest and fresh enough route to destination without checking the availability of routes and drops data packets without forwarding further, thereby degrading network performance.

Wormhole Attack

In a wormhole attack, an attacker receives packets at one end point in the network, tunnels data packets to another end point in the network, and then replays them into the network from that point. This tunnel between these end points cause two colluding attacks is known as a wormhole.

Replay Attack

An attacker which performs a replay attack is retransmitted the valid data repeatedly to cause network routing traffic that has been captured previously. This attack usually aims at the freshness of routes.

2. LITERATURE SURVEY

Jing Deng, Varshney.P.K, Balakrishnan.K The basic idea of the 2ACK scheme is to send two-hop acknowledgment packets in the opposite direction of the routing path. To reduce extra routing overhead, only a few of the received data packets are acknowledged in the 2ACK scheme. M. Nagaratna, V. Kamakshi Prasad, Raghavendra Rao This paper proposes the comparison of ODMR and PUMA protocol. As per the simulation results PUMA is better than ODMR. The primary goal of an ad hoc network routing protocol is to provide an efficient route establishment between a pair of nodes so that messages may be delivered in a timely manner. Route construction should be done with a minimum of overhead and bandwidth consumption. A.W. Moore and D. Zuev With the widespread use of mobile devices, the users of Mobile Ad hoc network (MANET) become increasingly more, which results the rapid development of the technology. Due to MANET don't need the infrastructure, it can deploy fast and conveniently in any environment. Because of its easy deployment features, in addition to used in personal area networks, home area networks and so on. Specially, MANET suit for military operations and the emergent disasters rescue that need to overcome terrain and special purpose in urgent. However the dynamical network topology of MANET, infrastructure-less property and lack of certificate authority make the security problems of MANET need to pay more attention.

3. METHODOLOGY

3.1 DTO METHOD

Dynamic Threshold Optimization (DTO) adaptively "compresses" the decision space (DS) in a global search and optimization problem by bounding the objective function. DTO is universally applicable, and the author believes it may be a novel approach to global search and optimization.

The thresholds are unsuitable for an environment with dynamic and unpredictable workloads, in which different types of applications can share a physical resource. The system should be able to automatically adjust its behavior depending on the work load patterns exhibited by the applications. Therefore, a novel technique for auto-adjustment of the utilization thresholds based on a statistical analysis of the historical data collected during the lifetime of VMs.

The CPU utilization created by each VM can be described by a random variable (uj) with a particular distribution, which persists at least over some recent period of time. In this case, the CPU utilization of a host can be represented by a random variable (Ui), which is a sum of utilizations by m VMs allocated to this host. The distributions created by dierent VMs are dierent, the distribution of the host's utilization is approximately normal and can be modeled by the t-distribution.

It cannot predict the CPU utilization of a physical node in the future to calculate characteristics of the distribution over some recent period of time, such as the sample mean (Ui) and standard deviation (sUi).

$$\overline{U_i} = \sum_{j=1}^{m} \overline{u_j}, \qquad s_{U_i} = \sqrt{\sum_{j=1}^{m} s_{u_j}^2}$$

The advantage of collecting the data for each VM separately and then using the summation is that a VM is migrated together with the data of its resource usage and the data will be actual even after a VM migration. Using this information and the inverse cumulative probability function for the t-distribution (tinvn(P)), it is possible tond out an interval of the CPU utilization, which will be reached with a low probability.

The upper utilization threshold (Tui) for each host i preserving this amount of spare CPU capacity dined by the lower (Pul) and upper (Puu) limits of the probability interval as shown in (6),where n is the number of data points collected, and n □ 1represents the degrees of freedom for the t-distribution. a low probability (e.g. 5%). The upper utilization threshold (Tui) for each

host i preserving this amount of spare CPU capacity denied by the lower (Pul) and upper (Puu) limits of the probability interval, where n is the number of data points collected, and n - 1 represents the degrees of freedom for the t-distribution.

$$T_{u_i} = 1 - ((t_{inv_{n-1}}(P_{uu}) \cdot s_{U_i} + \overline{U_i}) - (t_{inv_{n-1}}(P_{ul}) \cdot s_{U_i} + \overline{U_i}))$$

The lower threshold is calculated in a similar way; however, the deference is that a single value is obtained for all the hosts in the system. The idea is to determine the hosts that have lower utilizations relatively to the average value across all the nodes. To tackle the case when all the hosts have low CPU utilizations and to introduce a limit (Ul) to cap the decrease of the lower utilization threshold. In our previous have found the value Ul = 30% to be elective for the lower threshold.

$$\overline{U} = \frac{1}{N}\sum_{i=1}^{N}\overline{U_i}, \qquad s_U = \frac{1}{N}\sqrt{\sum_{i=1}^{N}(\overline{U_i} - \overline{U})^2},$$

$$T_l = \begin{cases} \overline{U} - t_{inv_{n-1}}(P_l) \cdot s_U, \text{ if } < U_l, \\ U_l, \text{ otherwise.} \end{cases}$$

The reallocation algorithm using the dynamic thresholds (DT) to find threshold value. For the DT algorithm apply the MM policy for VM selection, as in previous work it has shown the superiority over the alternatives. The complexity of the algorithm is proportional to the sum of the number of non over-utilized host plus the product of the number of over-utilized hosts and the number of VMs allocated to these over-utilized hosts.

3.2 GRA METHOD

A greedy routing anti void protocol is proposed to solve the void problem with increased routing efficiency by exploiting the boundary finding technique for the unit disk graph. A greedy anti-void (GRA) protocol is proposed to guarantee packet delivery with increased routing

efficiency by completely resolving the void problem based on the UDG setting. The GRA protocol is designed to be a combination of both the conventional GF algorithm and the proposed rolling-ball UDG boundary traversal (RUT) scheme. The GF scheme is executed by the GAR algorithm without the occurrence of the void problem, while the RUT scheme is served as the remedy for resolving the void problem, leading to the assurance for packet delivery. The GRA protocol to further enhance the routing performance with reduced communication overhead.

Greedy Forwarding

In the first mechanism, all data packets are forwarded to an adjacent neighbor that is geographically positioned closer to the intended destination. This mechanism is known as greedy forwarding. The forwarding is done on a packet to packet basis. Hence, minimal state Information is required to be retained by all nodes. It makes protocol most suitable for resource starved devices. However, this mechanism is susceptible to failure in situations where the distance between forwarding node and final destination is less than the distance between the forwarding node's adjacent neighbors and destination.

The performance of greedy routing for networks by providing bounds on the average delay and the average number of packets in the system for the dynamic routing problem. In this model packets are generated at each node according to a poisson process, and each packet is sent to a destination chosen uniformly at random. Our bounds are based on comparisons with computationally simpler queuing networks, and the methods used are generally applicable to other network systems.

4. EXPERIMENTS AND RESULTS

There are two flavors of Attacker attacks. In the first one, an attacker creates new identity while discarding its previously created one; hence only one identity of the attacker is up at a time in the network. This is also called a join-and-leave or whitewashing attack and the motivation is to clean-out any bad history of malicious activities.

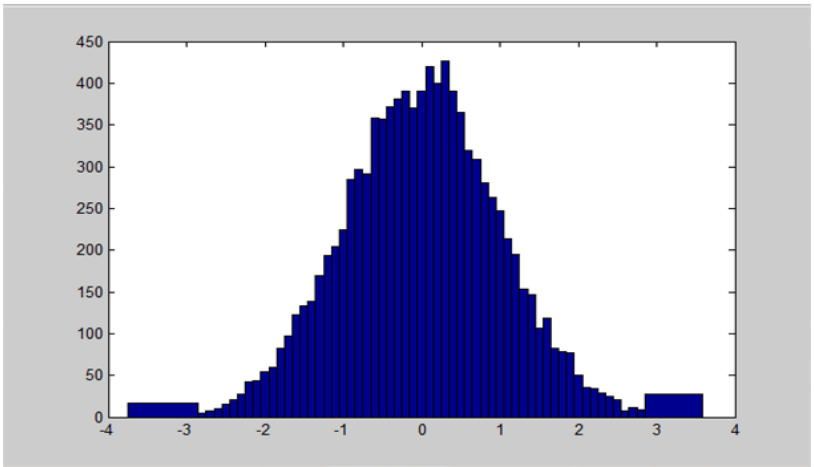
This attack potentially promotes lack of accountability in the network. In the second type of attacker attack, an attacker concurrently uses all its identities for an attack, called

simultaneous attacker attack. The motivations of this attack is to cause disruption in the network or try to gain more resources, information, access, etc. than that of a single node deserves in a network.

To setup our detection threshold based on the maximum speed of the network; assuming that no node can move faster than this maximum speed. This threshold will make the distinction because the first DTO from newcomers, if greater than the threshold imply abnormal entry into the neighborhood. Now the question becomes, which speed should adopt as the upper bound for our detection threshold. To answer this question and for clarity purposes, its logically partition the radio range of node A into two zones: a gray zone and a white zone.

The partitioning is based on the speed-based detection threshold. If the incorporate various speed-based thresholds, it would become clear that higher speed thresholds produce wider gray zones. Whitewashing in this area cannot be detected, since the first appearance (or acknowledgment) of a node in the gray zone would usually represent a normal entry into the radio range of the node.

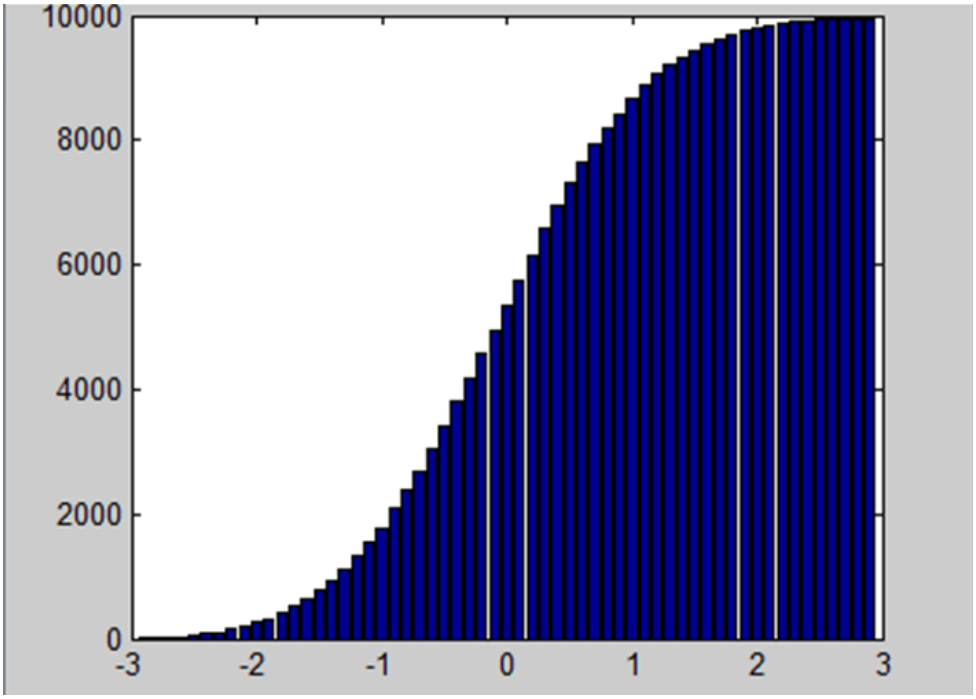
The intrusion detection is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized.



Malicious Node Ratio

Effect of Malicious Node on Packet Delivery Ratio

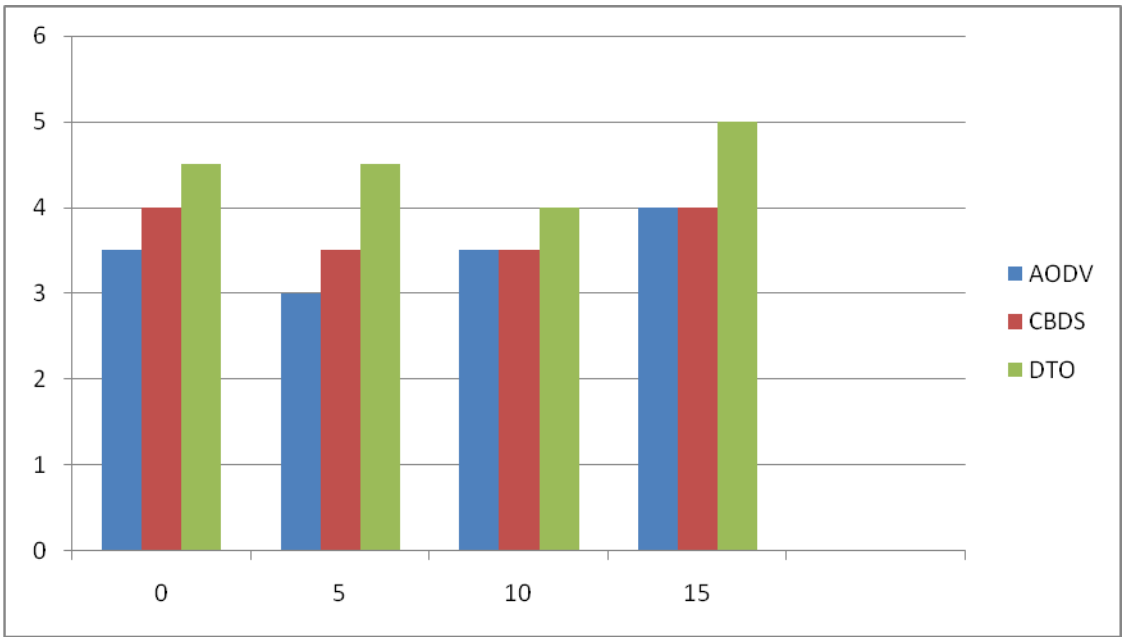
During simulation time the events are traced by using the trace files. The performance of the network is evaluated by executing the files. The events are recorded into trace files while executing record procedure. In this procedure, to trace the events like packet received, Packets lost, Last packet received time etc. These trace values are write into the trace files.



Packet Delivery Ratio

AODV is a reactive routing protocol that does not require maintenance of routes to destination nodes that are not in active communication. Instead, it allows mobile nodes to quickly obtain routes to new destination nodes. Every mobile node maintains a routing table that stores the next hop node information for a route to the destination node. When a source node wishes to route a packet to a destination node, it uses the specified route if a fresh enough route to the destination node is available in its routing table.

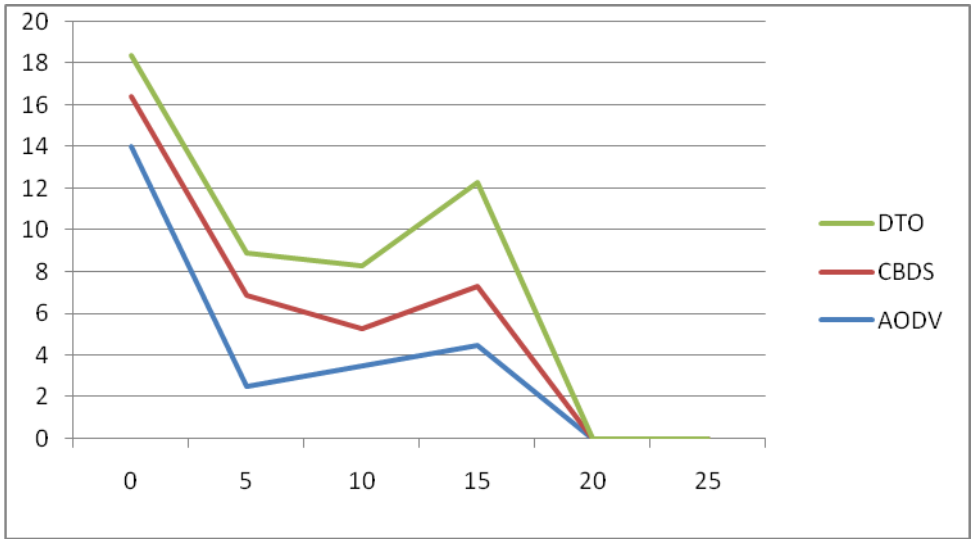
Here node from source to destination it will select the proper route and start to transmit the packets via intermediate nodes in the acknowledgement scheme. After packets received the destination, it will send the acknowledgment to the destination. If the source doesn't receive the acknowledgment source will decide may intruder attacks the intermediate node.



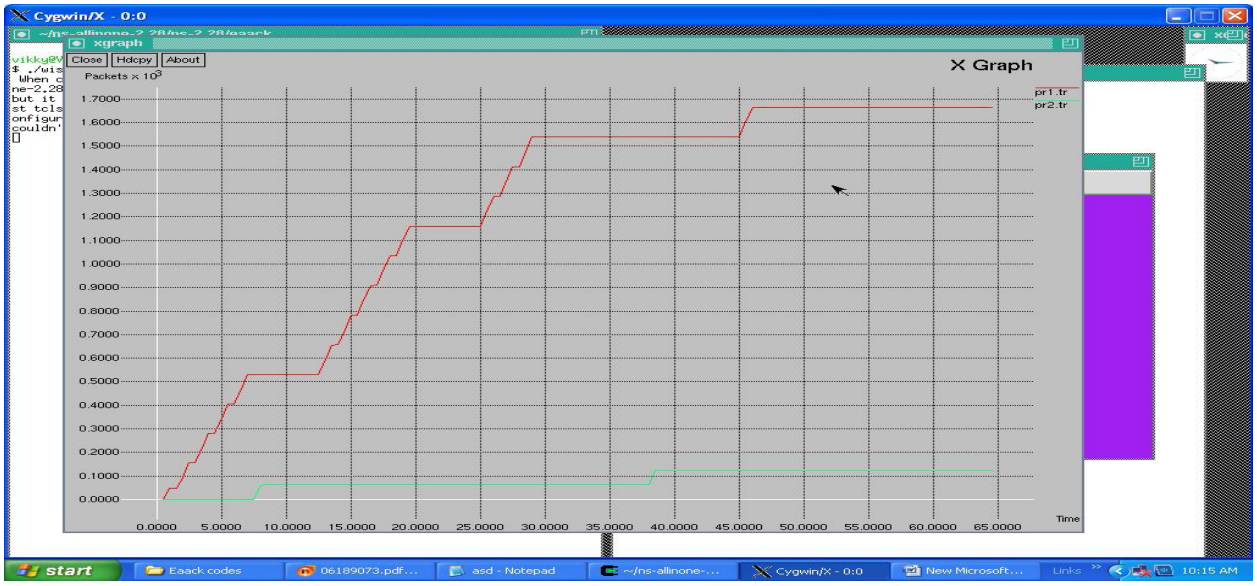
Speed(m/s)

Throughput for Different Thresholds

In the event of the absence of a black hole node, the total packet loss rates by AODV and MAODV are about 9.62% and 9.87%, respectively; with one fixed black hole node, the total packet loss rate rises sharply to about 90.42%. With the deployment of DTO nodes, the packet loss rate can be successfully reduced to about 15.7%.



The routing overhead of the CBDS reaches the highest value when the threshold is set to 95%. This is attributed to the fact that the detection scheme of CBDS triggers fast when the threshold value is 95% compared with when it is set to 85% or when it is equal to the dynamic threshold value. Thus, the bait packets will be sent many times in the network. It should be noticed that the dynamic threshold value can be adjusted according to the network performance.



Packet Transferred

The DTO yields a higher packet delivery ratio compared with CBDS. Finally, the DTO can detect malicious nodes successfully while keeping the packet delivery ratio above 90%. The maximum speed of nodes is varied from 0 to 20 m/s, and the percentage of malicious nodes is fixed to 20%. It is observed that the DTO can still detect malicious nodes successfully while keeping the throughput above 15 000 bit/s.

5. CONCLUSION AND FUTURE ENHANCEMENT

In this thesis, preventing or detecting malicious nodes launching grayhole or collaborative black hole attacks may lead to serious security concerns. Our proposed scheme use dynamic threshold optimization algorithm for detecting malicious nodes in MANETs under Gray/collaborative black hole attacks. It will automatically self configure itself to check the threshold value low or high before the data is sent. If the threshold value is high, no attacks are in

the node. If the threshold value is low means some malicious nodes are in MANET. The attacked node are removed and choose alternative path to send data to destination. It will automatically self-configure itself to check the threshold value low or high before the data is sent. The proposed approach can be use TCC, was proposed to investigate correlation information in real traffic data and incorporate it into traffic classification in a wide range of applications, such as automatic recognition of unknown applications from captured network traffic and semi supervised data mining for processing network packets.

REFERENCES

[1] T.Karagiannis, K.Papagiannaki, and M. Faloutsos, **"BLINC: Multilevel Traffic Classification in the Dark,"** Proc ACM SIGCOMM, vol. 35, pp. 229-240, Aug. 2005.

[2] T.T. Nguyen and G. Armitage, "**A Survey Of Techniques for Internet Traffic Classification Using Machine Learning,"** IEEE Comm. Surveys Tutorials, vol. 10, no. 4, pp. 56-76, Oct.-Dec.
2008.

[3] Y. Wu, G. Min, K. Li, and B. Javadi, "**Modelling and Analysis of Communication Networks in Multi-Cluster Systems Under Spatio-Temporal Bursty Traffic,"** IEEE Trans. Parallel Distributed Systems, vol. 23, no. 5, pp. 902-912, May 2012, http://dx.doi.org/ 10.1109/TPDS.2011.198.

[4] Y.-s. Lim, H.-c. Kim, J. Jeong, C.-k. Kim, T.T. Kwon, and Y. Choi, **"Internet Traffic Classification Demystified: on the Sources of the Discriminative Power,"** Proc. Sixth Int'l Conf. (Co-NEXT '10), pp. 9:1-9:12, 2010.

[5] Y. Xiang, W. Zhou, and M. Guo, **"Flexible Deterministic Packet Marking: An IP Traceback System to Find the Real Source of Attacks,"** IEEE Trans. Parallel Distributed Systems, vol. 20, no. 4, pp. 567-580, Apr. 2009.

[6] A.W. Moore and D. Zuev, **"Internet Traffic Classification Using Bayesian Analysis Techniques,"** ACM SIGMETRICS Performance Evaluation Review (SIGMETRICS), vol. 33, pp. 50-60, June 2005.

