ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

An Efficient Attack Resistance Model Using Application Based Polynomial Distribution

Vince Paul, Dr. K. Prasadh, Jasmy Davies

Research Scholar, Singhania University, Rajasthan, India .

Principal, Mookambika Technical Campus, Moovattupuzha, Kerala, India.

Assistant Professor & Research Scholar, Sahrdaya College of Engg. & Tech, Kodakara, Thrissur, Kerala, India.

ABSTRACT: Due to the increasing threat to the Internet on both popular Internet sites and Internet infrastructure, it is very challenging to provide reliable data transfer in a more secured manner for time-critical applications in an energy-efficient way. Several attack resistance schemes have been proposed to increase the effect of detection rate and the limitations of security, minimize the power overload, and energy consumption. However, they all disregard the time factor they take to accomplish the task of providing security and therefore miss significant opportunities for attack resistance. In this paper, we propose new approach called as the Application based Polynomial Distribution (A-PD) model for mitigating the problems related to application oriented DDOS attack. With carefully designed attack resistance strategies, A-PD model distributes the application services prior to sending the packet data streams. Since the distribution of packet data streams is performed in an efficient manner, the abnormality of service or the attack rate is minimized. The organization of packet data stream is performed using polynomial distribution according to the classification of application services using probability density function. The application of probability density function increases the detection rate and accordingly equate with the network traffic. Our techniques significantly outperform the state-of-the-art works. In comparison to prior work, our experimental results show that our model outperforms better in terms of detection rate, execution time, minimizing load overhead achieve. This, in turn, leads to improved security

KEY WORDS: DDos Attacks, Polynomial distribution model, attack resistance scheme, Network-level security and protection

I. INTRODUCTION

With the increasing growth in the Internet-based communities has made the intruders to interrupt the business processes at higher rate based on DDoS attacks. Without strong association holds, results with risk trailing customers, profits, and their fine status. But with the highly profitable e-business market, the efficiency, and universal achievement promote both consumers and businesses. But the convenience of today's business procedures provides with a higher rate of security confronts.

In a Denial of Service attack, the intruders or malicious users prevent the genuine users from admitting resources in a more sensible manner. Denial of service is also referred to as "the anticipation of approved access to a system source or the setback of system processes and functions." DDoS attack rapidly gets enter into the company's server, firewall, router or network link with traffic, if unsolved, the attack overflows the network or its resources. As a result, the entire genuine traffic cannot progress, followed by which the company cannot utilize the services provided to it. A security approach must directly recognize and react to DDoS threats, whereas preserving the accessibility of serious network resources on behalf of customers and employees. The DDoS attacks are described using Fig 1. Two user's user 1 and user 2 are shown with attacker A1 and attacker A2 represented in figure that attacks the application services.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

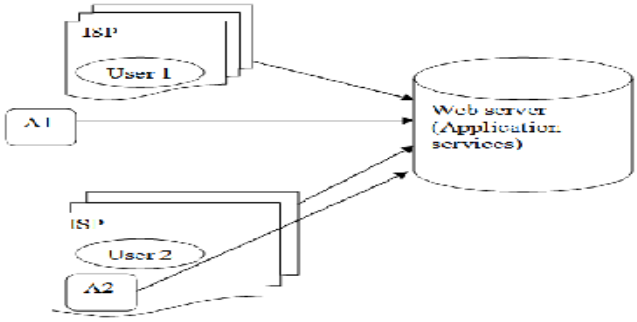

Fig. 1 DDoS attacks by attackers

In conventional form, the DDoS attacks were approved beyond the application layer, such as SYN flooding, ping of death attacks. The intention of these attacks is to deteriorate the network bandwidth by restricting the accesses to genuine users of the systems. Many researchers have observed such type of attacks and planned different methods and mechanisms, and have also provided solutions from bandwidth attacks.

Application layer DDoS attacks utilize genuine HTTP requests to submerge victim's possessions. Application layer may consists of one or arrangement of assembly flooding attack, demand flooding attack and asymmetric attack. By taking into account the bandwidth and processing control of application layer server, threshold for concurrently associated sessions and greatest number of requests that can be examined with declaration of Quality of service is determined.

Several distribution models have been used for attack resistance process to protect the service based approaches in network. The Polynomial distribution applied here is an overview of the binomial distribution. The design of binomial distribution is based on the amount of "successes" in *n* self-determining Bernoulli trials, with the similar prospect of "success" on each test. In a polynomial distribution, the analog of the Bernoulli distribution is the definite distribution, where every experiment results in accurately one of some predetermined limited number *k* of probable outcomes, and as a result there are *n* self-determining tests.

In this work we design an application based polynomial distribution model to mitigate against DDoS attacks. The attack resistance scheme is performed efficiently by balancing the load and then improving the security by distributing the application services prior to packet streaming.

II. LITERATURE REVIEW

One of the most common types of attacks observed in wireless sensor network is the denial-of-service (DoS) or distributed denial-of-service (DDoS) attack. This type of DDoS attack makes the reliable resources unavailable to the users who are intended to view at. DDoS attacks ranges from the temporary types of attacks to the most indefinite types of attacks affecting the Internet community. The main target of the intruders of DDoS attacks is to affect the most web servers to be of high profile in nature ranging from banks, financial institutions and so on at the application layer. Many efforts have been made to mitigate the DDoS attacks, but only limited works have been concentrated on application based DDoS attacks.

The main task of application based DDoS attack is that it interrupts the application services rather than disrupting the network. This application based DDoS attack in one of the major emerging problems that have to be solved when compared to the conventional types of DDoS attacks. A new model called as Group Testing (GT) [1] based to identify application based DDoS attack that not only included a model against conventional types of attacks but also reduced the low false positive/negative rate. However, the attackers were not isolated increasing the attack rate.

A new way of mitigating the DDoS attacks based on entropy variations called as EV [2] was designed that highly differentiated the normal and DDoS attacks using the technique called as the packet marking techniques. The method was proved to be highly scalable, robust and was in a way highly independent of different types of attack traffic

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

patterns. Though the method proved to be highly efficient for packet flooding, the classification regarding normal and higher attack rates were not discriminated posing higher security constraints.

With the rate of distributed denial of service (DDoS) attacks fetching to be more demanding with the immense resources and methods gradually are highly susceptible to attackers at a higher rate than ever before. Judge refined attacks [3] that are protocol-compliant, and employ genuine application-layer requirements overcome system resources. In [4] detection algorithms that highly detected the rate of DDoS attacks were designed and provided solutions to mitigate DDoS attacks. Moreover the theoretical complexity analysis was solved. But the method was highly susceptible to reputation or reliability. Spotting on the recognition for such new DDoS attacks, a method based on article reputation [5] was introduced.

Two novel metrics called as the generalized entropy metric and information distance metric was introduced in [6] to thwart against low rate DDoS attacks. But complexity increased with higher rate of DDoS attacks. A severe problem related to the network services are examined with respect to the application layer DDoS attack, and planned qualified entropy based app-DDoS detection method in [7]. A polynomial distribution used here for the distribution of application services can be applied for many characteristics. A DDoS attack can be a concurrent attack as designed in [12] on the association of the fatality (eg a web server or router) from a huge number of hosts that can extend between dissimilar networks and were distinguished independently in [13].

A new combined probability density function (pdf) methods based on the generalized Laguerre polynomial was designed in [8]. However, it faced a broad range of small-scale desertion distributions in wireless communications. In [9] cross-correlation examination was used in order to detain the market trends and identified in an efficient manner where and when a DDoS attack probably occurs and a DDoS flooding attack on jamming rapidly with respect to target of attack was designed in [10]. Gaussian distributed distribute component was newly proposed in [11] with the correct packet which is essential for wireless communications.

To improve the rate of communication, in [12] the characteristics of DDoS was analyzed and included a defensive mechanism to combat DDoS attacks. Though proved to be efficient, this method was not proved to be optimized. A new model for detecting application based DDoS attack was designed in [13] using entropy values of HTTP GET obtained through IP addresses increasing the scalability of attacks to be addressed. But the method was not proved to be securitized. To improve the security while mitigating DDoS attacks, a novel mechanism was introduced in [14] that used entropy as detection mechanism. A mobile and propagation type of DDoS was addressed in [15] using regulation based security model.

To improve the attack resistance scheme in wireless networks, in this work, we used polynomial distribution model for distributing the application services prior to the packet streaming to the destination from data source. The application based DDoS attacks are restricted using the distribution of services with polynomial distribution model.

III. APPLICATION BASED POLYNOMIAL DISTRIBUTION MODEL

The objective of application based polynomial distribution model (A-PD) is to develop an efficient attack resistance model that not only minimizes the attack rate but also to reduce the time taken to identify the rate of attack. Distributed servers have different types of application services that are highly susceptible to attack by the intruders at any possible time. As a result, in order to improve the rate of security in distributed server across the networks, an application based polynomial distribution model is introduced in this work.

The task involved in application based polynomial distribution model is to initially distribute the services at first, according to their types. As soon as the services are distributed and if any intruder or malicious nodes tries to hack or modify the services, then based on the abnormality the detection is made fast. Also the distribution of services across the network is also performed in an efficient manner using application based polynomial distribution model. With this, the distribution of services with packet data is equated according to the network traffic in order to ensure secure packet data transmission in an efficient manner. The architecture diagram of the proposed application based polynomial

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

distribution model to mitigate problems related to DDoS attack oriented to application services is illustrated in Figure 1.

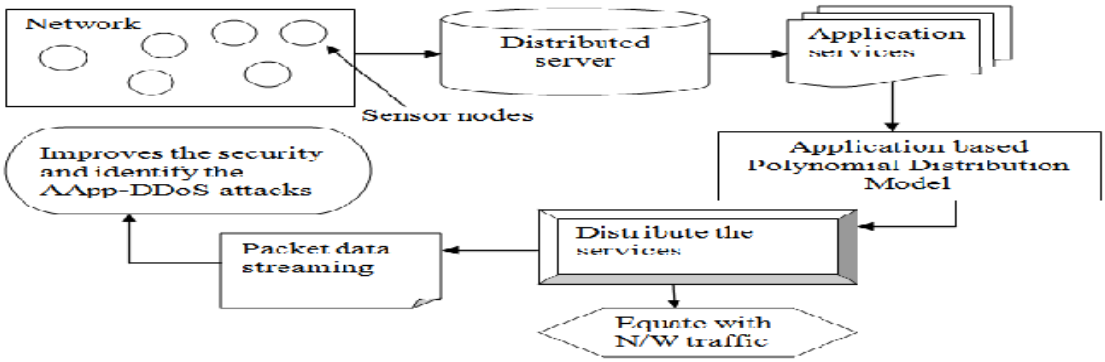

Figure 2 Architecture diagram of the proposed Application based Polynomial Distribution (A-PD) model

As shown in figure 2, a distributed server consists of several application services and these application services are highly susceptible to attacks known as Denial of service attacks. Usually, the attackers in the network initiate the DDoS attacks by following an immense amount of attack sources that launches an ineffective traffic to the victim. Upon identification of the application services, the polynomial distribution model is applied at this juncture that efficiently distributes the application services based on their classification.

The packet data streaming is used with the distribution of application services for efficient routing of packet data stream. This in turn eradicates the DDoS attacks based on the application services. For this successful accomplishment, the distribution of application services is equated according to the network traffic for resisting the attacks made by the intruders. The efficient design of attack resistance scheme for application based polynomial distribution model is briefly described in the forthcoming sections.

3.1 Application based Polynomial Distribution Model

The basic design considerations included in the formation of application based polynomial distribution model is that it identifies the attack by distributing information amongst contributing routers in the network. The objective behind application based polynomial distribution model is that it identifies the attack sources and to provide security to the modified packet data streams so that the server re-sources will be conserved. At the same time, the routers in A-PD model is more secured from attack sources and is capable or recognizing the attack in a more rapid and precise manner. When distributing a polynomial over any number of the sensor nodes in the network, the A-PD model distribute each node in the distributed server over followed by which the other nodes are distributed in the distributed server. When the distribution is completed, all the nodes in the network are combined together. According to the type of application services, they are classified for simplification.

Let us consider the sensor nodes $SN_1, SN_2, \ldots, SN_n$ in a network with different types of application services $AS_1, AS_2, \ldots, AS_n$ present in the network. Then the application services are classified according to their operation goal as given below

$$PD = (SN_1 + SN_2 + \cdots + SN_n)(AS_1 + AS_2 + \cdots + AS_n) = SN_1 (AS_1 + AS_2 + \cdots + AS_n) + SN_2 (AS_1 + AS_2 + \cdots + AS_n) + \cdots + SN_n(AS_1 + AS_2 + \cdots AS_n) \quad (1)$$

Upon successful completion of classification of application services, the application services are distributed along with the packet data streams $Disbn_{pds}$ using A-PD as given below

$$Disbn_{pds} = SN_1AS_1 + SN_2AS_2 + \cdots + SN_nAS_n \quad (2)$$

Finally, the application services which have the same packet data streams are combined together which results in the improvement of security.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

The application based polynomial distribution model for attack resistance scheme represents the probability distribution of the products obtained from the above polynomial experiment. The polynomial formula explains in detail about the probability of any product from a polynomial experiment.

Let us consider that the polynomial experiment consists of AS_n application services, with each application services resulting in any of PDS_k *k* packet data streams, $PDS_1, PDS_2, \ldots, PDS_k$. With each probable transmission of packet data stream transmission with probability $PR_1, PR_2, \ldots PR_n$, then the probability $PROB$ that PDS_1happens k_1 times, PDS_2happens k_2 times, and PDS_nhappens k_n time is described below

$$PROB = \left[\frac{k_1!}{(k_1!*k_2!*\ldots k_n)}\right]*(PR_1k_1 * PR_2k_2 * \ldots\ldots * PR_nk_n) \quad (3)$$

Polynomial distribution in A-PM is a form of distribution model in which the application services has been distributed based on its classification using the independent variable and the dependent variable is modeled as an *i*th order polynomial. To be more precise, the simplest form of distribution analysis measures and analyzes the attacks in application services. Based on the outcome variable and the deviation observed and the classification of application services, the rate of attack varies accordingly. Therefore, application based polynomial distribution model is an efficient tool that is used for the examination of changes in the network occurring between the sensor nodes.

3.2 Application based Polynomial Distribution representation for DDoS attacks

Once the application services have been classified the next step in A-PM is to identify or represent the DDoS attacks observed in the network. As the nodes in the network are exponentially increased in number, the difficulty is to design a model that is not only free from attack but also to identify the attack rate at minimal time. Given these constraints, the A-PM designs a polynomial factor $\pi\left(\frac{n}{c}\right)$ that is distributed over the space of application services.

An easy way to design A-PD model to mitigate application based DDoS attack is by substituting a polynomial factor over the entire network and then constructing independent paths from the distribution with substitution patterns according to the application services. The application services are distributed in such a way that it equates well with the network traffic and is also proportionate to the number of times the sensor node i was selected. With this strategy the polynomial distribution with the aid of polynomial factor is parameterized.

The exponential form used for A-PD model for a polynomial distribution with parameters Θ is given as,

$$PROB_\theta\ Density\ function\ (i) = \frac{AS^\theta}{z(\theta)} \quad (4)$$

Where $PROB_\theta(i)$ is the probability density function that the distribution serves all i nodes with the comparative value of Θ_i network traffic structure. With this a well structure distribution over n nodes for any value of Θ is observed.

3.2 Procedure for polynomial distribution model for attack resistance scheme

The polynomial distribution algorithm which has been used in A-PM model to mitigate application based DDoS attacks is given :

Step1: Identify the sensor nodes in the network

Step 2: Identify the application services present in the server

Step3: Using polynomial distribution model,

Step3.1 Distribute the services based on its classification and operational goal using (1) and (2)

Step 4: If attacker attacks the application services, then

Step 4.1: Application services abnormality easily identified based on the probability value identified from (3)

Step 5: Perform polynomial distribution using (4)

Step 6: Distribute the Application services in a minimal time and the security is improved using Polynomial distribution model representation

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Using (1) (2) (3) and (4), the efficiency of polynomial distribution model is achieved and solves the problem related to application based DDoS attack. With the application of polynomial factor and probability density, the security is improved. As the distribution of services is already performed prior to the packet data streaming, the services protected from abnormality is ensured. In addition with the network traffic characteristics equated with the distribution of application services, the user could identify the network traffic status and obtains optimal balancing of load carried.

IV. EXPERIMENTAL EVALUATION

The Application based Polynomial Distribution model (A-PM) in wireless sensor network performs experimental work on NS2 simulator. The movement of all sensor nodes is formulated over a size of 1000m x 1000m sensor field. NS2 simulation takes 200 sensor nodes for experimental purpose with the aid of DSR routing protocol to perform the experiment on randomly moving objects. The sensor nodes in the network move at the random speed of 100 to 800 m/s and an average pause of 0.05 ms.

Random Way Point (RWM) model is selected for move in a randomly chosen location. With the aid of RWM, the randomly selected nodes with randomly selected velocity provides with a predefined speed at a random progression rate which is observed to be constant during the simulation period. The selected sensor nodes with an arbitrarily selected speed contain a predefined amount and speed count. The Application based Polynomial Distribution (A-PM) model for mitigating the DDoS attacks in wireless sensor networks is compared against the existing Group Testing (GT) based approach [1] and Entropy Variations (EV) [2] on the factors such as entropy, processing time, load overhead and security.

The interval between two uninterrupted attack requests is determined on three samples counting stable rate attacks, growing rate attacks and arbitrary pulsing attacks. During the simulation, 120 nodes were observed in the process. There were twenty nodes termed as server nodes and remaining nodes were termed as client nodes. Attacker nodes were initiated when Server checkered client arbitrarily one by one.

The entropy in A-PM model derives the average amount of application services entered into the network drawn from a distribution or data packet stream. The entropy rate using A-PM model is given as the product of probability of applications services to logarithm form with based value c.

$$Entropy = H(AS_i) = -\sum_{i=1}^{n} PROB(AS_i) * \log c\ PROB(AS_i) \quad (5)$$

The processing time to identify the attack detection rate is the average time taken by a client node prior to the execution of an application server in the network and distributes the application services based on the classification. The processing time is the summation of time taken to perform polynomial distribution $Time\ (PD)$ and the time taken to perform distribution of packet data streams $Time\ (Disbn_{pds})$ as given below.

$$Proc_{time} = Time\ (PD) + Time\ (Disbn_{pds}) \quad (6)$$

The load overhead in A-PM model specifies the number of nodes in the network that are sent to the distributed server during a communication process. Security is measured in terms of percentage (%).

V. RESULTS AND DISCUSSION

In order to analyze the characteristics and functionality of the A-PM model, we quantitatively accessed the performance with the network size of 1000 * 1000 measured at 100 to 800 (m/s) using Dynamic Source Routing (DSR) Protocol by comparing the outcomes to the results achieved with the polynomial distribution algorithm. The Application based Polynomial Distribution (A-PD) model is compared against the existing Group Testing (GT) based approach [1] and Entropy Variations (EV) [2]. The experimental results using NS2 simulator are compared and analyzed with the help of table values and graphical representation as given below. To support transient performance, in Table 1 we apply an efficient polynomial distribution algorithm to obtain the entropy and comparison is made with two other existing techniques, GT andEV.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

Number of nodes (n)	Entropy (%)		
	A-PM	GT	EV
20	2.25	2.05	1.95
40	2.55	2.25	2.05
60	4.25	3.95	3.65
80	4.85	4.25	4.15
100	6.5	6.05	5.96
120	6.35	6.15	6.05

Table 1 Tabulation for entropy

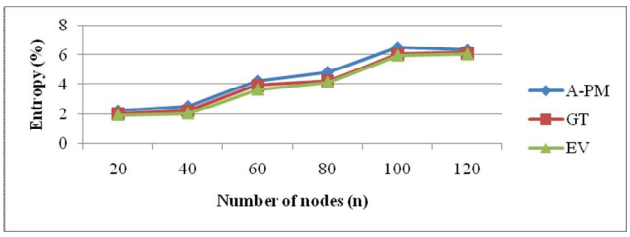

Figure 3 Measure of entropy using different nodes

Figure 3 show that the proposed A-PM model provides higher entropy rate when compared to GT [1] and EV [2]. This is because of the application of polynomial distribution model for each application services with respect to the number of nodes observed in the network through distributed server in A-PM model. It efficiently identifies the attack by distributing information between the routers based on the network traffic. As a result according to the application services classification is made according to the operational goal by providing higher amount of entropy rate by 3 – 11 % when compared to GT [1] and 4 – 19 % improvement compared to EV [2] respectively.

Number of nodes (n)	Processing time (ms)		
	A-PM	GT	EV
20	3.25	5.45	5.87
40	4.25	6.45	7.66
60	6.35	8.55	9.79
80	6.85	8.85	9.88
100	8.55	10.75	11.97
120	8.85	10.85	11.90

The comparison of processing time in terms of distribution of packet data streams is presented in table 2 with respect to the varying number of nodes with node density in the range of 10 – 80 at different speed. With increase in the number and size of nodes, the processing time for distribution of packet data streams is also increased.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

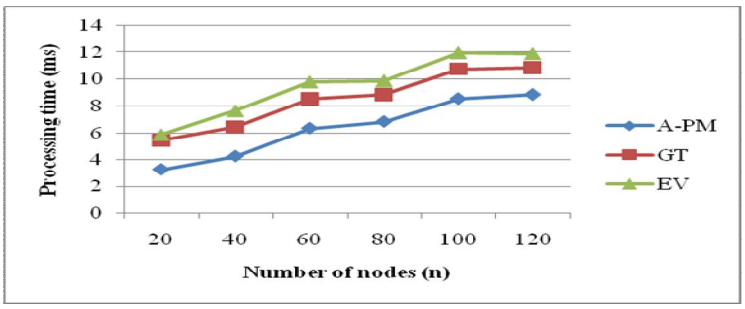

Figure 4 Measure of Processing time

To ascertain the performance of the processing time, comparison is made with two other existing works Group Testing (GT) based approach [1] and Entropy Variations (EV) [2]. In figure 4, the size of differing number of nodes is varied between 20 and 120 for experimental evaluation. From the figure 4 it is illustrative that the processing time taken to perform polynomial distribution and distribution of packet data streams increases with the increasing number of nodes. But comparatively lower using the application based polynomial distribution model. This is because with the differing sensor nodes and different types of application services, the A-PM model only the sensor nodes with the corresponding application services are combined for any number and size of nodes. As a result, the processing time is improved by 22 – 67% when compared to GT [1] and 40 – 87 % compared to EV [2].

Number of services	Load overhead (MB)		
	A-PM	GT	EV
2	245	366	412
4	275	396	425
6	320	441	565
8	345	466	585
10	425	546	614
12	450	571	685

Table 3 Tabulation for load overhead

The load overhead for A-PD model is elaborated in table 3. We consider the method with application services of range between 2 and 12 for experimental purpose using NS2 simulator. The outcome of the Application based Polynomial Distribution model (A-PD) for mitigating DDoS attacks is compared with the existing state-of-the-art works.

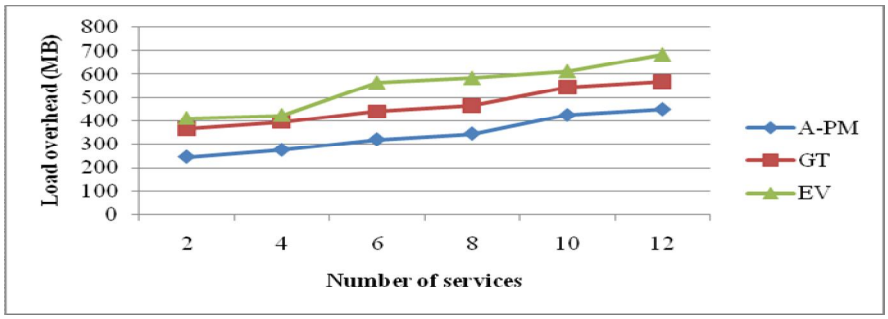

Figure 5 Measure of load overhead

Figure 5 describes the load overhead met when increasing number of nodes and services are used in the network using A-PD model and comparison is made with two other existing works. As the application services are distributed based on its classification using Polynomial Distribution model, the load overhead is comparatively observed to be of less in size using the A-PD model for application oriented DDoS attacks. The comparison result of load overhead for A-PD

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

model, mitigating against DDoS attacks with an existing GT and EV model is measured in terms of mega byte (MB). When number of services in the network increases, the service distribution overhead is less in the proposed A-PD compared to existing GT and EV by 26 – 49 % and 44 – 76 % respectively.

Methods	Security level (%)
Proposed A-PM model for application based DDoS attacks	74
Group Testing (GT) based approach	60
Entropy Variations (EV)	58

Table 4 Tabulation for Security level

The comparison of security level is presented in table 4 with respect to the different number of nodes and application services in the range of 20 – 120 and 2 - 12 respectively for experimental purposes using NS2 simulator. Elaborate comparison is made with two other methods, GT [1] and EV [2].

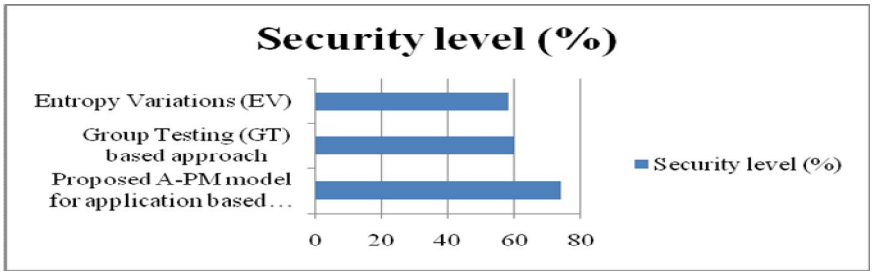

Figure 6 Measure of Security level

Figure 6 illustrate the security level versus the differing number of sensor nodes and application services measured in terms of percentage (%) for experimental purpose conducted using NS2 simulation. From the figure we can note that the security level is comparatively higher using the A-PD model than with the GT [1] and EV [2] model respectively. This is because application services which have the same packet data streams are combined together which results in the improvement of security. Furthermore, with the introduction of probability density function, polynomial distribution with parameters Θ, the application services are distributed in such a way that it equates well with the network traffic resulting in the improvement of security level by 18.91 % and 3.33 % compared to GT and EV respectively.

VI. CONCLUSION

An application based polynomial distribution model with differing sensor nodes and application services, have been designed to mitigate application oriented DDoS attacks in wireless sensor networks and to increase the security level. We adopt Polynomial Distribution algorithm, design and distribute the services based on the classification and operational goal with the probability density function handle the application services equating with the network structure. Thin in turn improves the security level and distribute the application services in a minimal time. The proposed attack resistance scheme is interoperable and reliable because of the eradication of application oriented DDoS attacks. In addition, the polynomial distribution model is developed as attack resistance scheme where the application services are distributed based on their classification prior to packet data streams that minimizes the processing time. Simulations were conducted with different sizes of nodes and application services to analyze the security on wireless network and measured the performance in terms of entropy, load overhead, processing time and security. Performances results reveal that the proposed A-PD model provides higher level of security and entropy and also strengthen security by consuming less processing time by mitigating against application based DDoS attacks. Compared to the existing

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 2, Issue 10, October 2014

state-of-the-works, the proposed Application based Probability Distribution model provides improvement in terms of security by 18.91 % and entropy by 19c% compared to state-of-art works.

REFERENCES

[1] Ying Xuan, Incheol Shin, My T. Thai, Member, IEEE, and Taieb Znati," Detecting Application Denial-of-Service Attacks: A Group-Testing-Based Approach", IEEE Transactions on Parallel and Distributed Systems, VOL. 21, NO. 8, AUGUST 2010
[2] Shui Yu, Member, IEEE, Wanlei Zhou, Senior Member, IEEE, Robin Doss, Member, IEEE, and Weijia Jia," Traceback of DDoS Attacks Using Entropy Variations", IEEE Transactions on Parallel and Distributed Systems, VOL. 22, NO. 3, MARCH 2011
[3] Ranjan, S, Swaminathan, R, Uysal, M, Nucci, A , "DDoS-Shield: DDoS-Resilient Scheduling to Counter Application Layer Attacks", IEEE/ACM Transactions on Networking, Vol.17, Issue.1, Feb 2009
[4] B. B. Gupta, Student Member, IEEE, R. C. Joshi, and Manoj Misra, Member, IEEE," Distributed Denial of Service Prevention Techniques", International Journal of Computer and Electrical Engineering, Vol. 2, No. 2, April, 2010
[5] Yi Xie, Guangzhou , Shun-zheng Yu, "Monitoring the Application-Layer DDoS Attacks for PopularWebsites", IEEE/ACM Transactions on Networking, Vol.17, Issue.1, Feb 2009
[6] Yang Xiang, Ke Li and Wanlei Zhou,"Low-Rate DDoS Attacks Detection and Traceback by Using New Information Metrics",IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY, VOL. 6, NO. 2, JUNE 2011
[7] Jin Wang, Xiaolong Yang, Keping Long, "A new relative entropy based app-DDoS detection method", IEEE Symposium on Computers and Communications (ISCC), Jun 2010
[8] Chin Choy Chai, Tjeng Thiang Tjhung , "Unified Laguerre Polynomial-Series-Based Distribution of Small-Scale Fading Envelopes", IEEE Transactions on Vehicular Technology, Vol.58, Issue.8, Oct 2009
[9] T. Peng and K. R. M. C. Leckie, "Protection from distributed denial of service attacks using history-based IP filtering," in Proc. IEEE Int. Conf. Commun., May 2003, vol. 1, pp. 482–486
[10] S.-Z. Yu and H. Kobayashi, "An efficient forward-backward algorithm for an explicit duration hidden Markov model," IEEE Signal Process. Lett., vol. 10, no. 1, pp. 11–14, Jan. 2003
[11] Zhan Yu, Chin Choy Chai, Tjeng Thiang Tjhung, "Envelope Probability Density Functions for Fading Model in Wireless Communications", IEEE Transactions Vehicular Technology, Vol.56, Issue.4, July 2007
[12] Shweta Tripathi, Brij Gupta, Ammar Almomani, Anupama Mishra, Suresh Veluru," Hadoop Based Defense Solution to Handle Distributed Denial of Service (DDoS) Attacks", Journal of Information Security, 2013
[13] Tongguang Ni, Xiaoqing Gu, Hongyuan Wang, and Yu Li," Real-Time Detection of Application-Layer DDoS Attack Using Time Series Analysis", Hindawi Publishing Corporation Journal of Control Science and Engineering Volume 2013
[14] Monika Sachdeva and Krishan Kumar," A Traffic Cluster Entropy Based Approach to Distinguish DDoS Attacks from Flash Event Using DETER Testbed", Hindawi Publishing Corporation ISRN Communications and Networking Volume 2014
[15] Claudio S.Malavenda,1 F. Menichelli,2 andM. Olivi," A Traffic Cluster Entropy Based Approach to Distinguish DDoS Attacks from Flash Event Using DETER Testbed Monika", Hindawi Publishing Corporation Journal of Computer Networks and Communications Volume 2014.

BIOGRAPHY

VINCE PAUL is a Research Scholar in the Computer Science and Engineering Department, of Singhania University , Rajasthan India. He received Master of Engineering (ME) degree in 2009 from VMKV University, TamilNadu, , India. His research interests are Network Security (Wireless and AdHoc Networks), Spoofing and DoS, Algorithms, and Artificial Intelligence , Neural Networks, Fuzzy Logic.