Asian Journal of Information Technology 15 (18): 3616-3623, 2016
ISSN: 1682-3915

An Enhanced Hidden Markov Dynamic Bayesian model for Resisting Camouflaging Worm attack study

[1]R.Saranya and [2]S.Senthamarai Kannan
[1]Department of CSE , Pannai College of Engineering and Technology, Sivagangai, Tamil Nadu, India
[2]Department of CSE, Pandian Saraswathi Yadav Engineering College, Sivagangai, Tamil Nadu, India

Abstract: At present, Camouflaging worm attack constitute a large part of internet peer servers. Due to the increasing traffic in internet services, it has become inevitable to take into account its effects on network management. Generally, studies on resisting Camouflaging Worm attack have involved analysis with power spectral density distribution via spectrum-based scheme. However, with several facilities provided by spectrum-based scheme, its network traffic volume in internet severs is increasing day by day increasing the malicious traffic rate. In this research proposal plan is to develop efficient identification of C-Worm propagation and restriction of uncontrolled malicious traffic in the internet by applying Enhanced Hidden Markov Chain-based C-Worm Detection (EHMC-CWD) technique. The C-Worm replicates the abnormal traffic on its own and propagates throughout the network and cause damages to the internet services. Enhanced Hidden Markov Chain (EHMC) identifies the camouflaging abnormal traffic replicated across the internet. Next, EHMC adapted a dynamic Bayesian network to evaluate camouflaging worm propagation by means of optimal non linear filtering. Therefore the replicated traffic generated by C-Worm reveals the information about the sequence of traffic in which it is propagated. The performance of EHMC-CWD is evaluated by extensive simulations. Simulation results show that our proposal can considerably reduce the execution time for C-Worm detection and memory space and also improves high detection rate to a certain degree.

Key words: Camouflaging worm attack internet services, spectral density, hidden markov chain, bayesian network, C-worm

INTRODUCTION

Providing security to the internet peer services has become an important issue due to the exponential increase in traffic and the mushroom growth rate of certain worms. The recent worm detection schemes are not able to scan and detect exponentially rising abnormal traffic patterns and become more vulnerable in providing security to internet peer servers.

Transmitting Adaptive Camouflage Traffic (TACT) (Lu *et al*., 2015) minimized message delay for timely smart grid communication under any potential jamming by applying Markov renewal process. To facilitate and detect C-Worm, Power Spectral Density (PSD) (Yu *et al*., 2011) distribution was applied in order to effectively detect the C-Worm propagation. However, the use of spectral model introduced potential congestion vulnerabilities due to the recurring multiplicative nature of C-Worm. A new model approach was developed (Xu *et al*., 2014) to estimate the P2P traffic matrices based on a close analysis of the traffic characteristic in P2P systems with improved accuracy. However, the computation of traffic matrix not straightforward and it is high measurement cost.

Abrantes *et al*. (2011), explicit congestion control algorithms were designed to improve the throughput. There have been extensive works on designing methods against resource depletion attacks which provide measures for sensing and pervasive computing. Measures were taken to mitigate vampire attacks (Vasserman and Hopper, 2013) by introducing coordinate and beacon state protocols on clean slate sensor network routing. However, recently, anti-collision protocols were introduced for single Reader Frequency based Identification (RFID). Porta *et al*. (2011), tree-based and aloha-based protocols were designed to improve the system time efficiency for detecting the attack. Cross layer jamming detection and mitigation was presented to mitigate the jamming effect on network.

Computer worms are one of the most serious threats to the Internet, causing huge amount of losses ranging in

Corresponding Author: R. Saranya, Department of CSE , Pannai College of Engineering and Technology, Sivagangai, Tamil Nadu, India

between billions to trillions of dollars. Vulnerability driven signatures (Wang *et al*., 2010) based on length-based signature generator was designed to reduce the polymorphic worm in internet. A road network based mix zone framework (Palanisamy and Liu, 2015) was designed that offered high level of anonymity reducing the transition attacks in an extensive manner. Another way to minimize the attack is to protect the location privacy. In (Mehta *et al*., 2012), source location privacy and sink location privacy was designed with the objective of improving the communication cost and latency.

To better portrait the features of C-Worm propagation in internet in this study, we study the normal behavior of the traffic and through it abnormalities are measured by constructing an Enhanced Hidden Markov Chain Based C-Worm Detection (EHMC-CWD) technique. Based on this technique, we analyze and restrict uncontrolled malicious traffic in internet through Bayesian Network-based C-Worm Detection algorithm. The remainder of the study is organized as follows: In Literature review, we introduce the background and review the related work. In Materials and Methods we introduce the Enhanced Hidden Markov Chain Based C-Worm Detection (HMC-CWD) technique. The performance evaluation results of our Markov Chain-based C-Worm detection technique are provided in Results and Discussion. We conclude this study in Conclusion.

Literature review: Our research relies on previous approaches for extending the most prominent Hidden Markov Model HMM and reduces the propagation of C-Worm in internet. Le and Markopoulou (2012), novel homomorphic MAC scheme called SpaceMac was used to minimize the computation overhead against pollution attack. Anti Blackhole Mechanism (ABM) (Su, 2011) on the other hand, presents an algorithm independent of the transmission model that rapidly block malicious node without false positive was provided. Another reputation-based protocol (Dini and Duca, 2012) was designed to reduce the black hole attack in the presence of delay tolerant network using acknowledgement, node list and aging mechanism.

Recently, a number of worm detection mechanisms have been developed for different types of networks. However, most of them are designed aiming at either improving the detection rate or latency. Shen peer-to-peer traffic matrices were analyzed and based on the analyzed traffic, network management was made in an efficient manner. On the other hand, to reduce the number of infected nodes, optimal distribution using content-based signature (Li *et al*., 2014, 2010) was investigated in mobile networks with heterogeneous devices. Optimal jamming attack and measures to mitigate using instantaneous payoffs was presented by Li *et al*. (2010). Intrusion detection is one of the most interesting areas in network due to the increase in the network traffic data. Balan *et al*. (2015), fuzzy based intrusion detection model was designed to provide a secure communication between nods. Spatial and temporal dynamics of worms were captured by Feng *et al*. (2015) to analyze worm propagation in network based on their equilibrium and stability. Worm attack is one of the severe threats to several networks. Most of the existing methods either require customized hardware or demand increased network overheads to extract the symptoms propagated by the worms which in result limits their applicability. Lu *et al*. (2015a, b), a passive worm detection and localization method was presented aiming at reducing the false alarms and detection latencies. To reduce the attack rate, password and distracter objects were used to improve the security issues (Ho *et al*., 2014). A picture-based password authentication method is uses a concept of concealing password information about the password images as much as possible. The password images selected by the users password identification phase used to verify the "target" image in the challenge set. But, the user input does not expose the password pictures to a shoulder-surfing adversary.

To alleviate the aforementioned problems, this work aims to propose a technique that is able to reduce the uncontrolled malicious traffic in the internet. The proposed technique is also able to identify the camouflaging abnormal traffic replicated across the internet. The following section explains the proposed technique in detail.

MATERIALS AND METHODS

Problem formulation: The primary goal of internet is to provide secured services to the internet users. Therefore, reducing the denial of internet peer server services is of critical importance and of which Camouflaging Worm (C-worm) that replicates and distribute the malware across the network by its own has to be identified. The C-worm attack did not require user intervention for spreading the false traffic, however spread on its own, and traffic flooding attacks increased exponentially. As a result, we focus on how to minimize the execution time for C-worm detection and the detection of C-worm at an early stage.

Enhanced hidden Markov chain: The C-worm refers to a malicious software program that propagates itself on the Internet and infects other hosts. The C-worm replicates

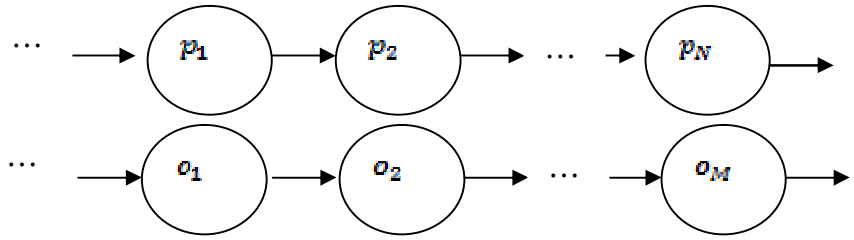

Fig. 1: Hidden Markov topology to measure malicious traffic

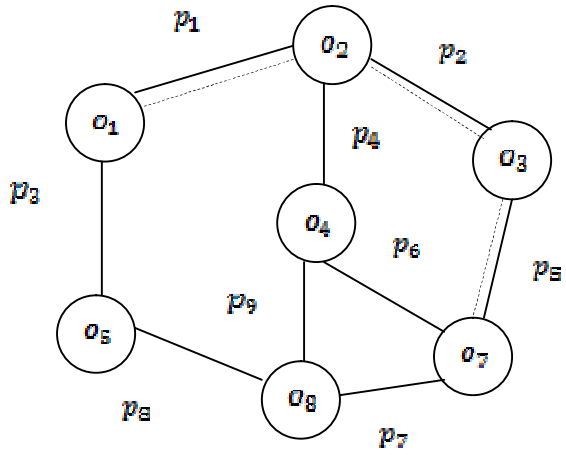

Fig. 2: Network structure with C-Worm attack

the abnormal traffic on its own and the propagation of the C-Worm is based on exploiting vulnerabilities of hosts on the Internet. The proposed work uses Enhanced Hidden Markov Chain (EHMC) to identify abnormal traffic replicated across the internet and restriction of uncontrolled malicious traffic in the internet. Here, hidden indicates the state of traffic which passed through the internet servers.

Based on this EHMC model an algorithm that measure the camouflaging abnormal traffic replicated across the internet by evaluating the distance between process monitored by abnormal traffic and normal traffic is presented.

Figure 1 shows the Hidden Markov model topology where $AN \in p_1,p_2,\ldots p_N$, and $B_M \in o_1,o_2..o_M$, represent the possible states and observations at time, t, respectively, with 'N and M' being the number of possible states and the observations in Internet.

From the Fig. 1 shown above, now the task is to analyze whether a camouflaging abnormal traffic is replicated across the internet and to measure the occurrences of network traffic (i.e. normal behaviour or anomaly behaviour) in the internet. In a network system monitored by a denial of service, the EHMC model monitors its runtime states described by a stochastic process through invisible finite Markov Chain, and the other through an observable Markov Chain with respect to the previous chain. Figure 2 shows a network structure with C-Worm attack.

As shown in Fig. 2, five observations 'o_1,o_2,o_3,o_4,o_5' and nine possible states '$p_1,p_2 \ldots p_9$' are figured out. An abnormal traffic is shown in dotted line that replicates the normal traffic, with propagation of C-Worm attack in the internet. With the objective of reducing the C-Work attack, an EHMC model is constructed in internet, whose state space includes two states, namely normal state 'NS = 0' and anomaly state 'AS = 1'. The observed chain is the sample of system behaviour or measure of malicious traffic in internet, where the system's state may belong to the normal state NS or anomaly state AS.

Let us construct an Enhanced Hidden Markov Chain model by considering a sequence of observations $O = o_1,o_2,..o_N$ on internet service IS where O IS. Then, the EHMC is described as given below.

$$\gamma = \left(HS_S, P, N, D, STP_{ij}, p, O\right) \quad (1)$$

From (1) HS_S refer to the size of hidden states and the size here denotes S = 2, where 0 denotes the normal state

and 1 denotes the ab normal state respectively. 'P' refers to the possible states, where P = $p_1,p_2,...p_N$, 'N' refers to the number of possible states, 'D' refers to the distribution of possible states, where D = {observer $_{system\ behaviour}$ = current $_{state}$ = i},'STP_{ij}' refers to the state transition probability, where '$[STP_{ij}]$ is denoted as below

$$\left[STP_{ij}\right]=\begin{bmatrix} STP_{00} & STP_{01} \\ STP_{10} & STP_{11} \end{bmatrix} \quad (2)$$

From (2), STPij = p{current $_{state}$ = i, next $_{state}$ = j} and p = $\alpha_1,..\alpha_N$ refers to the initial state probability given by study? = {α_1 α }$_{i2}$ = P{initial state} 'normal' and 'abnormal'state and 'O' being the observed possible state respectively. It is difficult to construct a model to identify the C-Worm propagating the abnormal traffic and restriction of uncontrolled malicious traffic in the internet as it is not directly visible and worm propagation differ significantly from one another.

The EHMC-CWD technique therefore constructs a model where abnormal behaviour is detected by its source variance on the internet with its state of dependency on the dynamic Bayesian network. This is studied by designing a model in such a way that more the distance of scan traffic volume, the more the probability that scan traffic volume data are generated by anomaly processes. Now let us define the state transition probability as given below.

$$STP=\begin{bmatrix} 1 & 0 \\ 1 & 0 \end{bmatrix} \quad (3)$$

From (3),the state transition probability STP in EHMC-CWD states that in a normal system behaviour, whatever the current state, the process or the system behaviour transfers to normal state next time by probability '1'.

Let the distribution of possible states in EHMC-CWD for normal system behaviour in the internet be denoted by 'D = 0' which states that the behaviour propagation under normal state condition are known, but the distribution of behaviour propagation under abnormal state condition is uncertain. Based on this Enhanced Hidden Markov Chain, the normal traffic is measured. The next step is to measure the possibility of malicious traffic in the internet. This is performed by designing a C-Worm detection algorithm provided in the following study.

C-Worm detection algorithm: Once the normal traffic is defined (as explained using EHMC), the next step is to design an algorithm to detect the C-Worm. The C-Worm detection algorithm starts with the ISC real-world trace provided by SANs ISC (Abrantes *et al*., 2011). Two steps are involved in the design of C-Worm detection algorithm. Initially, the probabilities of visible state sequence under the normal condition 'â'of the EHMC are obtained and are mathematically formulated as given below.

$$prob\left(\frac{0}{\beta}\right)=\sum_{i=1}^{n}\beta_t(i) \quad (4)$$

$$\beta_t(i)=prob(0_1,0_2,...,0_3) \quad (5)$$

From (4) and (5), '$o_1,o_2,..o_t$'represent the observed possible states until time interval 't' and 'i = 0|1' where 'i = 0 denotes normal state', and 'i = 1 denotes abnormal state', respectively. The second step determines whether an uncontrolled malicious traffic in the internet is detected or not based on the probabilities of visible state sequence.

In order to perform the C-Worm detection, the EHMC-CWD uses Higher Entropy Postulate (HEP) that when a sequence of traffic on the internet is running in normal state, the network traffic it generates contains less information than that it generates when running in anomaly state. Therefore, the network traffic entropy of malicious state is larger than that of normal state and so, the network traffic information entropy is used as the metric in identifying and detecting the C-Worm. EHMC-CWD adapted a dynamic Bayesian network to evaluate the camouflaging worm propagation by means of optimal non linear filtering to obtain network traffic information entropy. With EHMC-CWD, the self replicated C-Worm propagating the abnormal traffic which is not directly visible is detected with its state of dependency through dynamic Bayesian network. Each state of C-Worm propagation has a probability distribution over the possible traffic being replicated. Therefore the replicated traffic generated by C-Worm reveals the information about the sequence of traffic in which it is propagated.

With the sequence of observations generated by an EHMC-CWD that provides certain information about the state sequence, the Bayesian network is applied through which the decision regarding normal network traffic cost is arrived at:

$$TC_{ij}(0)=TC_{ij}\,Prob\left(\beta_t(i)/0\right) \quad (6)$$

Where 'O' is the observed state,'TC_{ij}' represents the network traffic cost of replicating the abnormal traffic from an observation of state 'O' to state 'j'and 'Prob (α_t(i) / O)'

symbolizes the posterior probability of a state. Followed by this the posterior probability of a state using Bayesian network is as given below:

$$\text{Prob}\left(\beta_t(i)/0\right) = N\,\text{Prob}\left(0/\beta_t(i)\right) * \text{Prob}\left(\beta_t(i)\right) \quad (7)$$

From (6) and (7) in this Bayesian network, the goal of EHMC model is to generate estimates of 'Prob (O / β_t (i))'from a classified set of available observations. Higher the variation higher the possibility of traffic being replicated is found to be. Let 'Avg(N)' represents the average network traffic entropy observed state sequences, and is formulated as given below.

$$\text{Avg}(N) = \sum_{i=1}^{n} \frac{\text{In prob}\left(\beta_t(i)/0\right)}{N} \quad (8)$$

Based on the value obtained from (8) the average network traffic entropy is used as a measure to distinguish between normal behaviour and anomaly behaviour. The C-Worm Detection algorithm based on Bayesian network mode. Particularly, the dynamic Bayesian network model assumes that any given host is in one of the following states: normal or abnormal. A normal traffic network is one that cannot be infected by a C-Worm, whereas the abnormal traffic network has the potential of being infected by a C-Worm through replicates. The objective now lies in efficient identification of C-Worm propagation and restriction of uncontrolled malicious traffic in the internetstudy.

With EHMC-CWD, the self replicated C-Worm propagating the abnormal traffic which is not directly visible, is detected by its source variance on the internet based on the state transition probability with its state of dependency on the dynamic Bayesian network. Each state of C-Worm propagation has a probability distribution over the possible traffic being replicated. Therefore, the probability of visibility state sequence, followed by normal network traffic cost and posterior probability is measured. Therefore the replicated traffic generated by C-Worm reveals the information about the sequence of traffic in which it is propagated through average network traffic entropy.

Bayesian Network-based C-Worm detection algorithm:

Input: Observations $0 = 0_1, 0_2 \ldots, 0_m$ possible states $p = p_{,1}p_{,2}\ldots, p_{,n}$ distribution of possible states. "D" state transition probability [STp_{ij}] initial state probability $p = \alpha_1, \alpha_2, \ldots, \alpha_n$, observed possible state "0"
Output: Optimized time and memory for C-worm
Begin
For each observations "$0 = 0_1, 0_2, \ldots, 0_n$"
Randomly choose "n" observation
Input training examples which consists of possible states "P"
For each state possible states "P"
Measure state transition probability using (3)
Measure probability of visible state sequence using (4)
Measure normal network traffic cost using (6)
Measure posterior probability of a state using (7)
Measure average network traffic entropy using (8)
End for
End for
End

RESULTS AND DISCUSSION

The Enhanced Hidden Markov Chain Based C-Worm Detection (EHMC-CWD) technique for efficient identification of C-Worm propagation and restriction of uncontrolled malicious traffic in the internet studies use the real-world Internet traffic traces (Shield logs data set) provided by SANs Internet Storm Center (ISC). In specific, the proposed EHMC-CWD technique used the ISC real-world trace (Shield logs data set) from 01.01.2005 to 01.15.2005. The purpose of using internet traffic traces is because of the gained popularity among the Internet security community in recent years.

In order to provide the creditability of data obtained from Shield logs data set by SANs Internet Storm Center, the traces were obtained from 20 day and measured the normal and abnormal traffic rate and simulations were conducted. Next, we conducted our simulation 7 times based on data randomly combined with different dates. The results, we showed in the study, are the mean values of experimental results from different rounds.

The experimental evaluation is conducted to evaluate the performance of proposed Enhanced Hidden Markov Chain Based C-Worm Detection (EHMC-CWD) technique with metrics such as size of normal data traffic and C-Worm replicated traffic, execution time for C-Worm detection, detection rate and memory space. The metrics were compared with the state-of-the-art methods namely, Transmitting Adaptive Camouflage Traffic (TACT) (Lu *et al*., 2015a, b) and Power Spectral Density (PSD) (Yu *et al*., 2011) for detection of C-Worm. The validation results are presented in three tables. Execution time for C-Worm detection is a measure to identify the time taken to detect the occurrence of C-Worm in internet. Therefore, the Execution time for C-Worm detection is the size of data traffic and the time taken to measure the posterior probability of a state using Bayesian network and is formulated as given below

$$\text{Time} = \text{DataTraffic}_s * \text{Time}\left(\text{Prob}\left(\beta_t(i)/O\right)\right) \quad (9)$$

From Eq. 9, the execution time 'TIme' measured is in terms of milliseconds (m sec). Lower the execution time

Table 1: Comparison of Execution time for C-worm detection

	Execution time for C-Worm detection (m sec)		
Size of data traffic (Mbps)	EHMC-CWD	TACT	PSD
150	158	174	188
300	175	191	205
450	192	208	214
600	205	221	227
750	224	240	256
900	248	264	280
1050	265	281	295

Table 2: Comparison of C-Worm detection rate

	C-Worm detection rate (%)		
C-Worm replicated traffic (Mbps)	EHMC-CWD	TACT	PSD
35	93.41	90.14	87.32
50	94.25	91.52	88.32
68	96.18	93.23	90.22
75	93.12	90.12	87.14
82	95.84	92.22	89.52
95	97.32	94.14	91.32
105	98.14	95.52	92.14

for C-Worm detection, more effective the method is said to be and higher the detection rate is said to be. Table 1 shows the results of the experimental validation of the proposed C-Worm detection technique against two other methods used in the literature Transmitting Adaptive Camouflage Traffic (TACT) (Lu *et al*., 2015a, b) and Power Spectral Density (PSD) (Yu *et al*., 2011) for detection of C-Worm.

Figure 3 describes the execution time for C-Worm detection with size of data traffic in the range of (150, 450, 750, 1050) Mbps. The decision point of data traffic was chosen in a random manner and was determined experimentally as that in which achieved a substantial improvement in ratings from the previous decision. The results show the superior performance of the proposed EHMC-CWD technique. The last values of the graph plotted in the figure seem to confirm the working hypothesis that the time for C-Worm detection increases with the increase in the data traffic size. As illustrated when compared to two other methods TACT (Lu *et al*., 2015a, b) and PSD (Yu *et al*., 2011), the EHMC-CWD technique substantially reduced the time for C-Worm detection using the extensive Enhanced Hidden Markov Chain. This is because the EHMC model adapted a dynamic Bayesian network that evaluated the camouflaging worm propagation through optimal non linear filtering, resulting in the improvement of execution time for C-Worm detection. Furthermore based on the distance between process monitored by abnormal traffic and normal traffic rate measured by its source variance on the internet reduces the execution time for C-Worm detection by 7 % compared to TACT and 13 % compared to PSD.

Table 2 shows the performance of C-Worm detection rate. Note that the gain by the new technique is

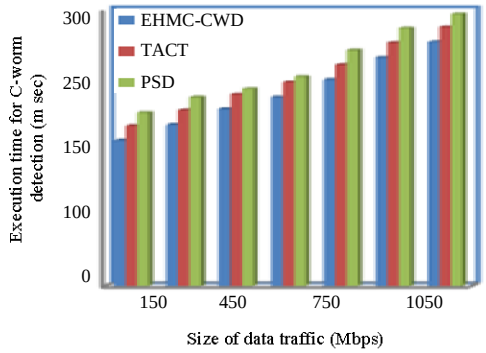

Fig. 3: Measure of Execution time for C-Worm detection

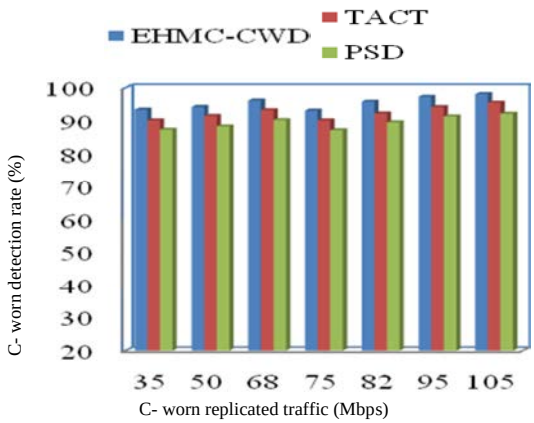

Fig. 4: Measure of C-Worm detection rate

consistent and overcomes the other C-Worm state-of-art detection methods in all states. The C-Worm detection rate is defined as the number of intrusion instances detected by the system divided by the total number of intrusion instances present in the test set.

$$D_{rate} = \frac{\text{Intrusion instance detected}}{(\text{traffic rate})*100 / Rep_t} \quad (10)$$

from (Eq. 10), the C-Worm detection rate D_{rate} is obtained by the traffic intrusion instances detected to the C-Worm replicated traffic rate Rep_t.

The C-Worm detection rate with respect to different C-Worm replicated traffic in internet using the EHMC-CWD technique and two methods, TACT and PSD are presented with visual comparison in Table 2. The results for different traffic rates with 35Mbps and 105Mbps are illustrated in Fig. 4. The C-Worm detection rate using our technique EHMC-CWD offer comparable values than the state-of-the-art methods. Results are

Table 3: Comparison of Memory space

Size of data traffic (Mbps)	Memory space (MB)		
	EHMC-CWD	TACT	PSD
150	610	678	723
300	845	705	755
450	1023	1083	1130
600	1058	1108	1158
750	1125	1185	1230
900	1148	1200	1250
1050	1176	1230	1280

presented for different sizes of C-Worm replicated traffic. Higher, the size of traffic, higher the detection rate is. This is because with higher traffic rate, the worm detection rate propagated in the network is easily analyzed based on the state space formulation. With the state space formulation, a stochastic process through invisible finite Markov Chain and observable Markov Chain with respect to the previous chain is obtained in an efficient manner. This in turn helps to detect the C-Worm propagation in the internet. The process is repeated with C-Worm replicated traffic size of 35Mbps to 105Mbps for conducting experiments. As illustrated when compared to two other methods TACT (Lu *et al*., 2015a, b) and PSD (Yu *et al*., 2011), the EHMC-CWD technique had better changes using the extensive dynamic Bayesian network. This is because in order to obtain better C-Worm detection rate, the Bayesian network applied in EHMC-CWD technique's that symbolizes the posterior probability of state. This in turn improves the detected rate by 3 % compared to TACT and 6 % compared to PSD. Memory for detecting C-Worm refers to the memory space required to detect the C-Worm. The memory is measured on the basis of the size of data traffic "Data Traffic$_s$" and the memory required for C-Worm detection Mem (D_{rate}) and is mathematically formulated as given below.

$$M = DataTraffic_s * Mem(D_{race}) \quad (11)$$

where (Eq. 11) memory M for detecting C-Worm are obtained in terms of megabyte (MB). Lower the memory, more efficient the method is. Table 3 represents the memory space required to detect the C-Worm in the internet using NS2 simulation and comparison is made with two other methods, namely TACT (Lu *et al*., 2015) and PSD (Yu *et al*., 2011).

The targeting results of memory space using EHMC-CWD technique is compared with two state-of-the-art methods (Lu *et al*., 2015), (Yu *et al*., 2011) in Fig. 5 is presented for visual comparison based on the size of data traffic. Our method differs from the TACT (Lu *et al*., 2015) and PSD (Yu *et al*., 2011) in that we have

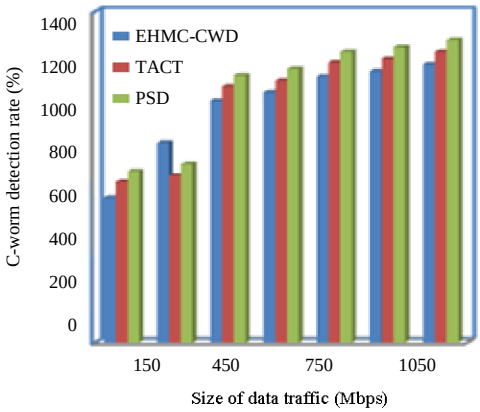

Fig. 5: Measure of memory space

incorporated C-Worm detection algorithm. By applying C-Worm detection algorithm for identifying the detecting the C-Worm attack in internet, the state transition probability and visible state sequence for each state is measured by applying a Higher Entropy Postulate (HEP). In addition, the extent to which a visible state sequence under the normal condition is included while measuring the normal network traffic using the posterior probability function. Therefore the memory space required to identify the C-Worm in internet is reduced by 2 % compared to TACT and 7 % compared to PSD respectively.

CONCLUSION

In this study, we provided a comprehensive study on minimizing the execution time for C-Worm detection across internet. By defining an Enhanced Hidden Markov Chain model, we showed that the execution time for C-worm detection is reduced by means of optimal non linear filtering. We designed a C-Worm detection algorithm by its source variance on the internet with its state of dependency on the dynamic Bayesian network, to improve the C-Worm detection rate in a significant manner. We present simulation results to support our theoretical results and show that C-Worm detection rate can be effectively improved and therefore reduces the damages caused to the internet services.

REFERENCES

Abrantes, F., J.T. Araujo and M. Ricardo, 2011. Explicit congestion control algorithms for time varying capacity media. IEEE. Trans. Mob. Comput., 10: 81-93.

Balan, E.V., M.K. Priyan, C. Gokulnath and G.U. Devi, 2015. Fuzzy based intrusion detection systems in MANET. Procedia Comput. Sci., 50: 109-114.

Dini, G. and A.L. Duca, 2012. Towards a reputation-based routing protocol to contrast blackholes in a delay tolerant network. Ad Hoc Netw., 10: 1167-1178.

Feng, L., L. Song, Q. Zhao and H. Wang, 2015. Modeling and stability analysis of worm propagation in wireless sensor network. Math. Prob. Eng., 2015: 1-9.

Ho, P.F., Y.H.S. Kam, M.C. Wee, Y.N. Chong and L.Y. Por, 2014. Preventing shoulder-surfing attack with the concept of concealing the password objects information. Sci. World J., 2014: 1-13.

Le, A. and A. Markopoulou, 2012. Cooperative defense against pollution attacks in network coding using spacemac. IEEE. J. Sel. Areas Commun., 30: 442-449.

Li, M., I. Koutsopoulos and R. Poovendran, 2010. Optimal jamming attack strategies and network defense policies in wireless sensor networks. IEEE. Trans. Mob. Comput., 9: 1119-1133.

Li, Y., P. Hui, D. Jin, L. Su and L. Zeng, 2014. Optimal distributed malware defense in mobile networks with heterogeneous devices. IEEE. Trans. Mob. Comput., 13: 377-391.

Lu, L., M.J. Hussain, G. Luo and Z. Han, 2015. Pworm: Passive and real-time wormhole detection scheme for WSNs. Intl. J. Distrib. Sens. Netw., 2015: 1-17.

Lu, Z., W. Wang and C. Wang, 2015. Camouflage traffic: Minimizing message delay for smart grid applications under jamming. IEEE. Transac. Dependable Secure Comput., 12: 31-44.

Mehta, K., D. Liu and M. Wright, 2012. Protecting location privacy in sensor networks against a global eavesdropper. IEEE. Trans. Mob. Comput., 11: 320-336.

Palanisamy, B. and L. Liu, 2015. Attack-Resilient mix-zones over road networks: Architecture and algorithms. IEEE. Trans. Mob. Comput., 14: 495-508.

Porta, T.F.L., G. Maselli and C. Petrioli, 2011. Anticollision protocols for single-reader RFID systems: temporal analysis and optimization. IEEE. Trans. Mob. Comput., 10: 267-279.

Su, M.Y., 2011. Prevention of selective black hole attacks on mobile ad hoc networks through intrusion detection systems. Comp. Commun., 34: 107-117.

Vasserman, E.Y. and N. Hopper, 2013. Vampire attacks: Draining life from wireless ad hoc sensor networks. IEEE. Trans. Mob. Comput., 12: 318-332.

Wang, L., Z. Li, Y. Chen, Z. Fu and X. Li, 2010. Thwarting zero-day polymorphic worms with network-level length-based signature generation. IEEE/ACM. Trans. Networking, 18: 53-66.

Xu, K., M. Shen, Y. Cui, M. Ye and Y. Zhong, 2014. A model approach to the estimation of peer-to-peer traffic matrices. IEEE. Trans. Parallel Distrib. Syst., 25: 1101-1111.

Yu, W., X. Wang, P. Calyam, D. Xuan and W. Zhao, 2011. Modeling and detection of camouflaging worm. IEEE. Trans. Dependable Secure Comput., 8: 377-390.