Enhanced Cooperative Agent Framework with Security and Increased Performance of the Computer Network

Hemraj Saini
Department of computer Science & Engineering / ICT
Jaypee University of Information Technology, Waknaghat, Solan-173234
hemraj.saini@juit.ac.in,
hemraj1977@yahoo.co.in

Kapil Dev Sharma
Department of CSE
Swami Keshvanand Institute of Technology Management & Gramothan, Jaipur-302025
skmkapil@gmail.com,
skmkapil@yahoo.com

T.C.Panda
Department of Applied Mathematics
Orissa Engineering College,
Bhubaneswar-752050
tc_panda@yahoo.com

***Abstract*— Every computer network needs some of the mechanism to protect itself against the malicious attacks. The common process for this is to divide the whole network into various coverage areas. Every coverage area elects its coverage agent who is responsible to collect the malicious information from its coverage area and share it with the other coverage areas. This will help to protect the computer network against malicious attacks.**

The core for this process is cooperative agent framework and enhancement of it will lead to increase in the security & performance of the computer network. The paper deals to enhance the cooperative framework in respect of the security of the function of cooperative agent as it will be having the more degree of the sensitivity of the malicious attack.

Keywords*— *Cooperative Agent, Computer Network Performance, Malicious Attack, Coverage Area, Cyber Security, Cooperative Agent Framework

I. INTRODUCTION

There are many literature [1, 2, 3] available which use cooperative agent for information sharing to protect the computer network against the malicious attacks. [4] proposed a cooperative framework for virus defense where different coverage areas have to be considered and for every coverage area there is a coverage agent (CA). These coverage agents are to be used for the following different purposes-

a. Coverage of a CA decides in rank order whether to actively scan for the virus or not.

b. CA exchanges the information about the state of the virus with other CAs.

c. CA determines the polling rate to maximize the probability of seeing enough virus to confirm the current local estimate of the virus.

In the continuation of the above work a significant enhancement in the cooperative process among CAs has been proposed in the current text. The main point which is to be considered here is the security aspects about the functioning of CA. The CA has the responsibility to collect the malicious attack/traffic from its coverage area and further to share it with other CAs with a cooperative process. Therefore, it is having the more degree of malicious attack over itself as compare to other members of coverage area because once a CA is identified by the cyber attacker then it may be attacked by it for the maximum loss. After the attack over a CA, the whole previously collected information by it can be destroyed for its coverage area. The coverage area elects its new CA and collects the whole information again. This process will be the overhead in the functioning in the computer network and degrade the performance. This is depicted in the following figure-1(a) and (b)-

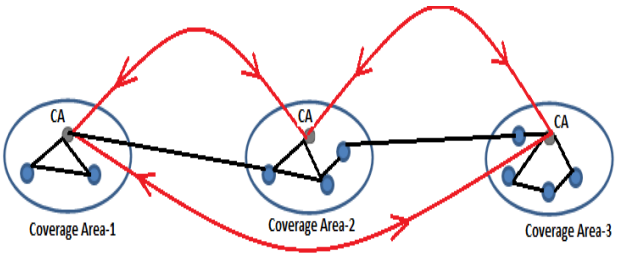
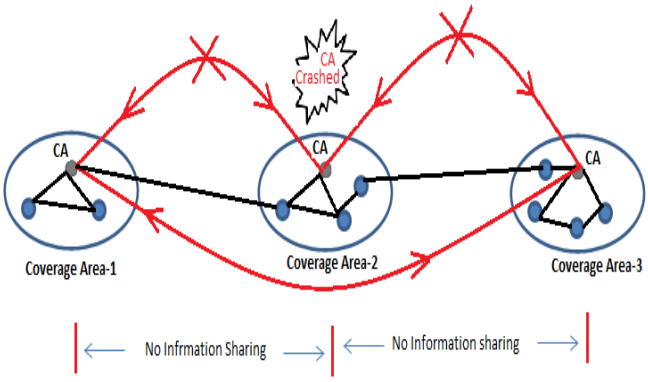


Figure-1: CAs for different coverage areas and information sharing



F

Figure-2: CA of coverage area-2 crashed and no information sharing in (coverage area-1 to coverage area-2) and (coverage area-2 to coverage area-3)

In this approach the information related to the crashed CA will be vanished as depicted in figure-2. The crashed of the CA leads to the corresponding coverage area to select the new CA. This new CA will not be having any previous information and

978-1-4673-5986-3/13/$31.00 ©2013 IEEE

need to collect all the information from the new forthcoming interactions. Therefore, lots of time and resources have to be consumed.

II. PROPOSED SOLUTION

To decrease the degree of sensitivity of a coverage agent a schema has been proposed i.e. after a random amount of time the coverage area agent has been replaced by another node. This timer amount, let us say, is τ. In this process the coverage area agent has to transfer the whole amount of information to the new coverage area agent. This process increases the overhead to the computer network. To reduce this overhead the information transfer will not takes place immediately but in a next Δτ time duration. This time duration has been chosen by such a way that the old and new coverage agent has less load of communication during Δτ. The old coverage agent has to do little extra responsibility to transfer the information as well as to consult with the new coverage agent. If there is information sharing with other covering agent in Δτ. This process can be directed in the following figure:-

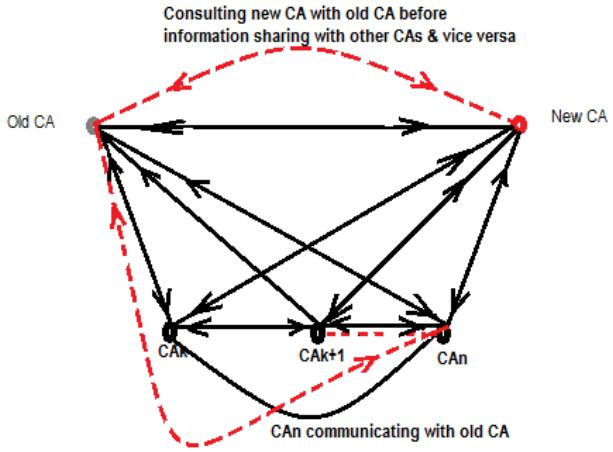


Figure-3 (a): Process during Δτ to transfer the information for new CA

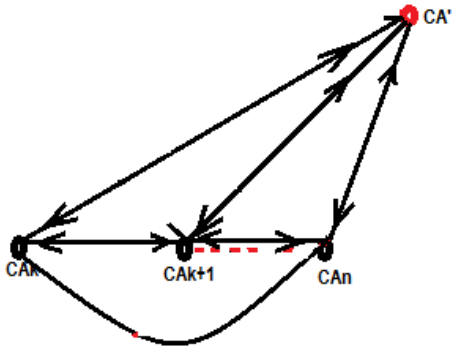


Figure-3 (b): Situation after complete information transfer within Δτ duration

After the transfer of complete previous information to new CA the old CA becomes the simple node of that coverage area.

III. MODELING OF THE PROPOSED APPROACH

The proposed approach can be better explained with a model. Assume that a computer network has P number of computer nodes. In the computer network various correlated areas, coverage areas, have to be created. This task can be accomplished with the help of k-means algorithm [5, 6, 7, 8].

Each identified reason by the k-means algorithm represents a coverage area in the computer network. Let there are N coverage areas after applying the k-means algorithm. Each coverage area needs to share the information with others through a CA. Therefore, each coverage area has to undergone a process of selection of a CA from its members on the basis of minimum or almost no outgoing traffic from it. The process is assumed stochastic and follows the Binomial process because the coverage area is variable due to the crashing of nodes (rare) or adding new incoming nodes.

A. Brief Description Of K-Means Algorithm

Suppose that we have n sample feature vectors $x_1, x_2, ..., x_n$ all from the same class, and we know that they fall into k compact clusters, k < n. Let m_i be the mean of the vectors in cluster i. If the clusters are well separated, we can use a minimum-distance classifier to separate them. That is, we can say that x is in cluster i if $|| x - m_i ||$ is the minimum of all the k distances. This suggests the following procedure for finding the k means:

- Make initial guesses for the means $m_1, m_2, ..., m_k$
- Until there are no changes in any mean
  - Use the estimated means to classify the samples into clusters
  - For i from 1 to k
    - Replace mi with the mean of all of the samples for cluster i
  - end_for
- end_until

Here is an example showing how the means m_1 and m_2 move into the centers of two clusters as shown in figure-4.

Figure-4: Showing the means m1 and m2 move into the centers of two clusters.

B. Brief Description of Binomial Process

The probability that a random variable X with binomial distribution B(n, p) is equal to the value k, $Pr(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$, where k = 0, 1,....,n , is given by , where $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

The latter expression is known as the binomial coefficient, stated as "n choose k," or the number of possible ways to choose k "successes" from n observations [9, 10, 11, 12].

Every coverage area elects its CA by following the Binomial process. Elected CA starts its communication with other members of the coverage area and collects all the occurred malicious information from them to share outside the coverage area through the CA of other coverage area and enrich it's as well other CA's information about the malicious attack. The probability of a node to be elected as CA in the network where the change of rate of coverage area is λ can be given by following equation-

$$\Pr(X = k) = \binom{n}{k} p^k (1-p)^{n-k}$$

Later on after a certain amount of time again the current CA initiate the random process to elect the new CA. As soon as the new CA is elected it transfers its collected information to the new CA and itself becomes the member of the same group. This process will be repeated after each certain amount of time.

C. Analogy: Watchman System of A Street

The benefit of the approach can be understood be the analogy of the safety of a city. In a city, there are Areas and Streets. Suppose each street has its own responsibility of security. The process of the steered security can be like follows-

Randomly select a hose to provide a night watchman of age in between 25 to 35. This watchman collects the important information about the night to night information related to theft and the way of other safety hazards.

After a certain period say, one month, the another family is randomly selected to provide the next watchman. This process eliminates the treat of the lost of the information collected by the watchmen. Information may lost if the watchman is too old and died or mixed with the thieves. After election of the new watchman, the old one has to transfer all the collected information the newer one.

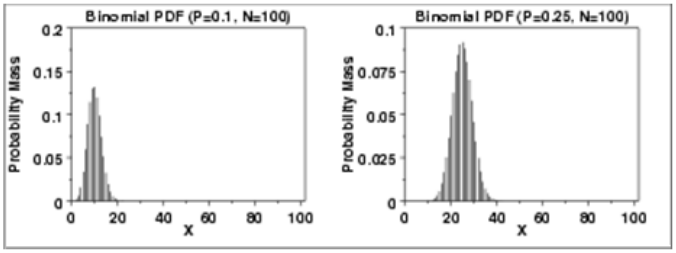


Figure-5: Depicts the probability mass function of a node K to be CA for different two (02) values of p, 0.1 & 0.25, if the minimum traffic at that time is considered in a network of N=100 nodes.

Figure-5 depicts the probability mass function of a node K to be CA for different two (02) values of p, 0.1 & 0.25, if the minimum traffic at that time is considered in a network of N=100 nodes.

IV. PROS AND CONS OF PROPOSED ENHANCED COOPERATIVE AGENT FRAMEWORK

Table-1 represents the pros and cons of proposed enhanced cooperative agent framework. The framework increases the defense against the known attacks as it shares the knowledge of others. Unknown attacks can also be identified first time by some members and share to others so that they can also defend against them, hence improved defense against unknown attacks. There will be no loss of collected malicious information but almost negligible reduction may be there in the processing.

TABLE-1: PROS AND CONS OF PROPOSED ENHANCED COOPERATIVE AGENT FRAMEWORK.

Particulars	Bad
Defense against known attacks	Best
Defense against unknown attacks	Improved
Loss of collected malicious information in the network	No loss
Speed of processing in the network	Negligibly reduced

V. CONCLUSION AND FUTURE WORK

The cooperative agent framework and enhancement of it is provided which is lead to increase in the performance of the computer network and security against the malicious attacks. The deployment of the proposed framework is also explained step by step with its pros and cons.

In the future the framework has to be extended to overcome the negligible reduction of the speed and to fully secure the network against the newly developed malicious attacks in the real environment.

REFERENCES

[1] P. E. Clements, R. M. Jones, R. H. Weston, and E. A. Edmonds. 1995. A framework for the realization of cooperative systems. SIGOIS Bull. 15, 3 (April 1995), 9-10.

[2] Clements, P., Coutts, I.A., & Weston, R.H. A life-cycle support environment comprising open systems manufacturing modelling methods and the CIM-BIOSYS infrastructural tools. MAPLE '93, Ottawa, Canada.

[3] Gengxin Miao, Shu Tao, Winnie Cheng, Randy Moulic, Louise E. Moser, David Lo, and Xifeng Yan. 2012. Understanding task-driven information flow in collaborative networks. In Proceedings of the 21st international conference on World Wide Web (WWW '12). ACM, New York, NY, USA, 849-858.

[4] Dashun Wang , Zhen Wen , Hanghang Tong , Ching-Yung Lin , Chaoming Song , Albert-László Barabási, Information spreading in context, Proceedings of the 20th international conference on World wide web, March 28-April 01, 2011, Hyderabad, India

[5] Rupali Vij and Suresh Kumar. 2012. Improved k- means clustering algorithm for two dimensional data. In Proceedings of the Second International Conference on Computational Science, Engineering and Information Technology (CCSEIT '12). ACM, New York, NY, USA, 665-670.

[6] Chih-Cheng Hung and Mojia Sun. 2010. Ant colony optimization for the K-means algorithm in image segmentation. In Proceedings of the 48th Annual Southeast Regional Conference (ACM SE '10). ACM, New York, NY, USA, , Article 48 , 4 pages.

[7] Amiya Halder and Avijit Dasgupta. 2012. Image segmentation using rough set based k-means algorithm. In Proceedings of the CUBE

International Information Technology Conference (CUBE '12). ACM, New York, NY, USA, 53-58.

[8] Bikram Keshari Mishra, Amiya Rath, Nihar Ranjan Nayak, and Sagarika Swain. 2012. Far efficient K-means clustering algorithm. In Proceedings of the International Conference on Advances in Computing, Communications and Informatics (ICACCI '12). ACM, New York, NY, USA, 106-110.

[9] Shanti S. Gupta and Gary C. McDonald. 1983. On using selection procedures with binomial models. In Proceedings of the 15th conference on Winter Simulation - Volume 2 (WSC '83), Stephen Roberts, Jerry Banks, and Bruce Schmeiser (Eds.), Vol. 2. IEEE Press, Piscataway, NJ, USA, 473-474.

[10] Constantinos Daskalakis, Ilias Diakonikolas, and Rocco A. Servedio. 2012. Learning poisson binomial distributions. In Proceedings of the 44th symposium on Theory of Computing (STOC '12). ACM, New York, NY, USA, 709-728.

[11] Gianni Amati and Cornelis Joost Van Rijsbergen. 2002. Probabilistic models of information retrieval based on measuring the divergence from randomness. ACM Trans. Inf. Syst. 20, 4 (October 2002), 357-389.

[12] Voratas Kachitvichyanukul. 1983. Discrete univariate random variate generation. In Proceedings of the 15th conference on Winter simulation - Volume 1 (WSC '83), Steve Roberts (Ed.), Vol. 1. IEEE Press, Piscataway, NJ, USA, 179-188.