Detection ofMalicious Behaviour ofAgent Using Attack Detection Strategies underMultiagent System

Supriya More[1], Sharmila Gaikwad[2]

P.G Student, Department of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India

Assistant Professor, Department of Computer Engineering, Rajiv Gandhi Institute of Technology, Mumbai, India

**Corresponding Author:Supriya More*

ABSTRACT: Multiagent system become more and more widespread due to successful implementations in different fields. However, there are a number of threats that can compromise security of the agent and jeopardize systems security. Security issues should be taken into consideration during expansion of multiagent system. Different surviving methodologies that provide guidelines and models for development of multiagent systems omit security. Therefore, there is a great need in offering security solutions which are integrated with system functionalities. This research presents a model for multiagent system and security under multi agent system. Moreover, possible attacks under multiagent system by malicious agent such as Denial of Service attack and Man in Middle attack are discussed. For detection of attack various algorithm such as correlation of coefficient and adaptive threshold algorithm is implemented. Using markov method depending upon attacker agent state, defense state is carry out and malicious agent get block. Finally, Stability Analysis under multiagent system using Lyapunov's method is discuss.

KEYWORDS: DoS attack, MAS, Man in Middle attack, Markov process, stability analysis

Date of Submission: 27-04-2018 Date of acceptance: 12-05-2018

I INTRODUCTION

Now a days, Agent technology plays an important role in the development of many major service application. Multiagent systems (MAS) are famous for their ease of use and utility in sharing and examining for content or Multiagent used to share utility to collect information from various nodes and for that coordination is required means they have to agree on decision, this decision is also known as consensus [1],[2],[3]. MAS are distributed and concurrent and the agents that makeup a MAS is able to exhibit complex, flexible behavior in order to achieve its objective in the face of dynamic and uncertain Environment [4]. Multiple agents interact with each other to accomplish the goal of the network. There are many such networks in the real world. They are part of grid computing, Peer to Peer (P2P) network and so on. Distributed coordination of networks of dynamic agents has concerned a number of researchers in recent years. There are various applications of MAS are present in several area, such as cooperative control of unmanned air vehicles (UAVs),online medical diagnosis system, formation control flocking, distributed sensor networks, attitude alignment of clusters of satellites, and congestion control in communication networks as mentioned in [1],[2],[5].Agent based systems have been widely developed in open distributed environments, especially in electronic commerce, mobile computing, network management, and information retrieval areas.Agent characteristics are as follows:

a. Agent responds in a timely manner to changes in the environment.
b. Agent keep fits control over its own actions.
c. Agent does not act in response to the environment.
d. Agent is continues running process.
e. Agents communicate to other agents and systems.
f. Agent can change its behaviour's based on preceding experience.
g. Agent can migrate from one machine to another.
h. Agent actions may not be scripted.

Mobile agents are software that can migrate from node to node in computer network and perform a computation on the behalf of the user [6]. The MAS like peer to peer (P2P) are vulnerable to security attacks as they are anonymous, open and dynamic in nature. Some agents may get compromised and act like malicious agents. They pamper the secure communication over the network. Hence, a MAS is affected. As mention in [7] and [8], there are two different attack scenarios in a MAS, first attack is on the dynamic behaviors (or closed-loop dynamics) of the agents and second attack is on the communications among the agents. Both of attacks can dramatically affect the consensus properties of the whole team. Under the assumption that the network is complete, consensus problem was studied in [1, 2] for MAS with adversaries. An attack on a specific node is identical to node removal on network so that connectivity restoration mechanism studied in [2]. The great challenge is balancing between implementation of advance feature of agent and maintaining security within MAS. In [9], researcher come up with trust evolution model that evaluates the behavior of parties to help in making the decision of who to interact with. In open environment, a platform must prepare for deliberate attack, from outside as well as inside. Malicious agent typically attempt to gain access to resources on a host they are not authorized to use. Such access include attempts to access private data of the host, private data of other agent or to use additional computational resources that have been negotiated. As studied in [1, 2], malicious agent do connectivity maintain attack or connectivity broken attack. In [10], the author mention attacks on Agents affecting communication such as Man in the middle, Denial of service attack, Reply attack on agent communication. To maintaining cyber strategy, for each state of attacker agent, the system should have defense state. Hence, detection of attack is key of defense. By this secure control framework will designed.

II DETECTION OF STRATEGIC ATTACKS UNDER MAS

1.1 Attacks

Attacks are distinguish between two forms of attacks, first is active attacks and second is passive attacks. Passive attacks are mainly based on observation without altering data or compromising services, they represent the interception and interruption forms of security threats. In contrast, active attacks alter or delete data and may cause service to be denied to authorize users. They represent the modification and fabrication forms of security threats. Typical active attacks attempt to modify or destroy files. Communication related active attacks attempt to modify the data sent over a communication channel. When attack is carried out by malicious agent, communication is blocked to the point that the agent cannot receive or transmit any information to the rest of the team, this disrupts the group objective [11]. The main objective of this research paper is detection of denial of service (DoS) attack and Man in the Middle (MITM) attack by malicious agent from the inside of MAS.

1.1.1 Denial of Service Attack

In [12], Denial of Service attacks are defined as attacks that are launched by a set of malicious entities towards a victim, with the aim of incapacitating it from providing further service to legitimate clients. DoS attacks involves the flooding of a channel with messages so that access is denied to others. DoS attacks are intended to shut down the MAS for a period of time [13]. Content of message is changed and saved file with unreadable format. A DDoS attack is a distributed form of denial of service attacks. DoS attacks consume the resources of a remote host or network by sending large numbers of IP packets over a short time period. Denial of service attack destroys the data availability in control system [2]. To initiate DOS attack, in [14] three mechanisms are used.

a) Attack on protocol: The attacker can take advantage of the security risk lying in the protocol to deplete the resource of the victim.

b) Attack on infrastructure: The Automatic metering reading (AMI) system built on the Intrusion Detection System (IDS) is a packet exchange network where the routers play an important role.

c) Attack on bandwidth: The attacker can manipulate a large number of agent to send excessive communication packets to the victim. In MAS malicious agent add data traffic over system. Denial of service attack result in operational overload so that target system crashes [15].

1.1.2 DOS Attack detection using Correlation of IP Address Analysis.

This section present attack detection scheme as studied in [16].

1.Analyze the abnormal traffic within MAS using correlation coefficient.

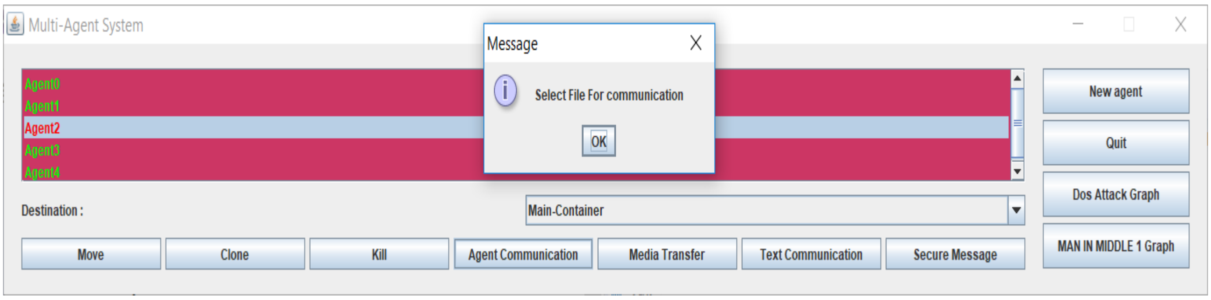
2.Calculate amount of data to be transferred by Agent.

3.Attacker or malicious agent added some amount of data into file while communication, which is detected by using correlation coefficient.

4.Calculate packet rate per second send by agent.

5.If traffic where added in the file by the agent or it beyond to limit, then DOS Attack is detected.

6.Otherwise continuous execution.



Select File For communication

Fig 1. Multiagent System

Fig 1 shows MAS with agent named as Agent0, Agent1, Agent2, Agent3, and Agent4. This agents can be move or clone themselves to or within different container. Here Agent 2 is select file for communication if Agent 2 add traffic then Agent 2 will consider as malicious agent.

Algorithm 1: Based on [16], DOS Attack Detection using Correlation of IP address analysis steps are as follows:

1. X_i (n) indicates the amount of data packets sent by i-th agent in the n-th sliding window time interval over platform.

$$X_{i\,(n)=\sum_{k=1}^{3} X_i\,(n_k)}(1)$$

2. Then move the slide window one unit time interval rightward, statistic the number of data packets sent by agent in the next slide window time interval X_i(n+1) and the total amount of data packets sent by all IP addresses X(n+1)

$X_i(n)\ =$

$\sum_{k=n}^{3+n} X_i\ \ (n_k)$ (2)Calculate the mathematical expectation of number of data packets of every IP address in a slide window time interval.

$$E(X(n))=X_i(n)\frac{X_i(n)}{x\ (n)} \qquad (3)$$

$$S=S+\ [X_i[n]\text{-}EX[n]]*[X_i\ [n+1]\text{-}EX\ [n+1]; \qquad (4)$$

$$DX[n] = DX[n] + [X_i[n] - EX[n]]\hat{}2 \qquad (5)$$

$$DX[n+1] = DX[n+1] + \big[X_i[n+1] - EX[n+1]\big]\hat{}2; \qquad (6)$$

3. Calculate the correlation coefficient of packets in adjacent slide window time intervals using the correlation coefficient formula over multiagent platform's IP address.

$$\rho_{xy} = S/(sqr(DX[n]) * sqr(DX[n+1])(7)$$

It will helpful to find out Misuse Detection as abnormal network Traffic using correlation coefficient in MAS.

1.2 Man-In-The-Middle (MITM) Attack under MAS

A man-in-the-middle or man-in-the-center assault is a sort of digital attack wherever the aggressor covertly transfers and potentially changes the correspondence between two gatherings who believe they are straightforwardly speaking with each other. MITM assaults are to a great extent recognized, or avoided by two means, first is confirmation and second is harm location. Confirmation gives some level of an assurance that a given message has originated from a source. Methods for alter discovery, by correlation, just shows confirm that a message may have been adjusted, instead of giving any certifications. Cryptography is used in the data communication system to secure the information. Differential Fault Analysis (DFA) is powerful means to jeopardize implementation of embedded cryptography. In DFA attacker agent provokes faults during the execution of cryptographic algorithm in order to extract information about the secret by analysing the differential effect on the output. The errors that are introduced during implementation of cryptographic algorithms are called as fault injection attack. In Advanced Encryption Standard (AES) during encryption, it accept a plaintext. 128 bit Key is specified to generate cipher text. Many authors introduced series of simulation for evaluation of robustness of unprotected AES algorithm against fault injection attack. During implementation of Asynchronous Encryption System (AES) one or several faults are injected and faulty output is used to obtained information [17]. In MAS malicious agent who act like man in middle, listen and alter data while communication. Hence, there is need of implementing strategy for detection of man in the middle attack. Following algorithm is useful for man in middle attack detection.

1.2.1 Detection of Man in The Middle attack in MAS

Algorithm 2: Detection of MIMT Attack

Input: Agent List, Msg

Output: Encrypted Msg

```
Key Size: 128 bit (16 byte)
Round: 4-Round
Begin:
Show AgentList Li;
Pick Agent form Li;
Write (Msg);
Send to Listener;
Select 128 bit key value;
Encrypt (Msg);   //perform
Execute AES;
                    If (Msg content Changed)
                              {
For (int i :readchar[i]))
Show misuseDetection=count of file;
Display: Attack Detected;
                              }
                    else{Continue communication ;}
```

III ATTACK DEFENDER MECHANISM USING MARKOV METHOD

Intrusion detection system (IDS) is a type of security mechanism for computer network. In [18], the research presented a system to accelerate and facilitate the process of analyzing data traffic by using agent working in parallel and distributed through various host system. In [19], IDS is defined as host based detection or as network based detection. It can be used as anomaly detection or as misuse detection. An intrusion is unauthorized access to the network through which an intruder can steal or modify user data from the system. Intrusion detection system design for detecting the unauthorized intrusion and attacks by knowing and doing studies about network behavior, security log by auditing data set and internet information [20]. Model based resilient control algorithm that enable the team of autonomous agents accomplish their formation task even the presence of a malicious denial of service (DOS) attack disrupting inter agent communication has been shown in [12]. To achieve resilient control, when an attack is detected, the state of the model is used to determine the control action for the agent and the corrupted information coming through the network is ignored. When an attack is detected, agent locally determine their control action based on state values provided by the identified system discarding value coming through network[21]. Formation control in MAS heavily relies upon accurate information exchange between agents. The tight integration of system physical infrastructure with computational and communication infrastructure make MAS susceptible to malicious attack targeting both physical and communication infrastructure. To achieve secure control, in [21] authors proposed distributed adaptive approach employing a local observer the estimate the state of an agent under normal system operation and uses this information to ensure resilient control in the presence of misbehaving agent.

For intrusion detector mechanism in MAS, this research paper consider state of each agent using Markov process. Markov process is define as follows.

Definition 1: A stochastic process is a sequence of event in which the outcome at any stage depends on some probability [22].

I Definition 2: A Markov process is a stochastic process with following properties [23].
II The number of possible outcome or state is finite.
III The outcome at any state depends only on the outcome of previous stage.
IV The probabilities are constant over time.

Algorithm 3. Attack defender Mechanism using markov process

```
1. Start
2. Execute Markov process
3.  Check Event type (Active, Inactive)
4. If (event Request = Active&& assign task execute) then no intrusion under MAS
5. If (event Request = Active&&Attack executes) then select protection action
6. End if
7. End if
```

To check whether agent is in active state or not first markov process is execute. Output of Markov process is agent state prediction, which is either active or not. If current agent is active then is returns 1, or if agent is inactive then it returns -1. If agent is active and doing his own task means agent is not misbehaving within

MAS. If agent is not doing his task and doing strategic attack under MAS then using markov decision policy attack detection and protection action is made.

2. Detection of Malicious Behaviour of Agent Using Adaptive Threshold Mechanism

This section consider algorithm that prevent and block behaviour of malicious agent. Detection of malicious agent speak about the problem of finding the anomalous activity in MAS. The anomaly detection system controls the abnormality by measuring the distance between the anomalous activity and normal activity based on chosen threshold [20]. When this procedure is followed, increases the throughput by preventing intruders. This reduces the computational time of the system and maintains the throughput and bandwidth. Adaptive threshold is measure network traffic and compare it with previously defined threshold. A threshold that is adaptively set using recent traffic measurements. If measured traffic exceed a particular threshold it will be defined as anomaly [7]. In such abnormal MAS, administrator needs to investigate and block the network traffic before serious damage occur in MAS [24].During the detection phase the detection subsystem called the incoming packets within a frame. The collected packets are subjected to blacklist. If packets is listed in blacklist, the detection will send the packets directly to the prevention subsystem without further processing. If a packet is considered to be normal, the detection system will send the packets to its destination [25].

The value of the threshold is set adaptively based on an estimate of the mean number of packets which is computed from recent traffic measurements. The value of Mean, Median, and Max is based upon Alpha, Beta, and Gamma as mention in following expression (8, 9, and 10). Based on [26], following steps are used to calculating Alpha, Beta, and Gamma.

1. Calculate value of Alpha

Alpha is the value calculated using (no_of_packets - threshold)/ threshold, as shown in expression (8). Parameter alpha is tuning parameter by chosen value after every particular time interval.

$$\alpha_n = \frac{X_n - T_n}{T_n} \qquad n=1, 2, 3 \qquad (8)$$

Where $\alpha > 0$ and Xn > Tn

n : number of intervals time

Xn : no. of packets

Tn: value of threshold

2. Calculate Value of Beta

Calculate beta for every particular time interval using following expression (9)

$$\beta_n = \frac{2}{X_{n+1}} (9)$$

3. Calculate Value of Gamma

Calculate mean after every particular time interval for every protocol using following expression (10)

$$\bar{\mu}_n = \left(\left(\overline{\mu_n} - 1 * \beta_n\right) + \left(1 - \beta_n\right) * x_n\right)(10)$$

Depending upon mean, median, Max value misuse detection is calculated.

Algorithm 4. Calculating Adaptive Threshold

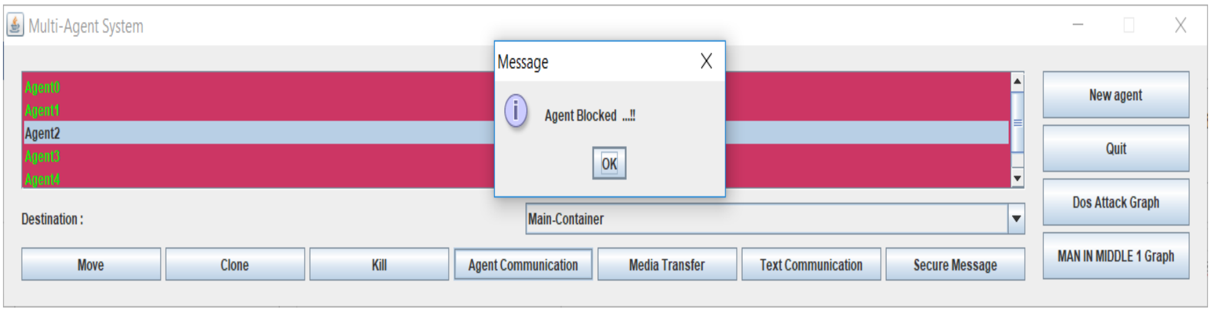
1. Initialize one variable as counter i.e. k
2. If the number of packet exceeds these threshold increase counter by 1.
3. When it repeated k times, then malicious behaviour of agent is detected.

Algorithm 5. To block malicious agent

After detection of malicious behaviour of agent, that agent id is store in intruders list and block that agent.

```
1. Start
2. If (event_Request = Active) then executes assigned task successfully
3. If (DOS||MIMA executes) then Check Intruders List, add agent id and  block the agent /*Ignore the request*/
4. else if ( selected agent is already blocked)  then check Authenticated Agent's List /*Ignore  the request*/
5. else (Accept the  request) and (Start communication)
6. end if
7. end if
```

Following Fig 2shows, malicious agent get blocked after DoS attack detection.



Agent Blocked ...!!

Fig.2 Block Agent

3. Stability Analysis And Attack Frequency

A piecewise quadratic Lyapunov function is explored, which is determined by solving an algebraic Riccati equation (ARE) and an algebraic Riccati inequality (ARI). Solutions of an ARE and ARI, a procedure to select the control gains is provided. Lyap solves the special and general forms of the Lyapunov's matrix equation. X = lyap (A, Q) solves the Lyapunov's equation, where A and Q are square matrices of identical sizes (shown in expression 11 and 12). X = lyap (A,B,C) solves the generalized Lyapunov equation (also called Sylvester equation).The matrices must have compatible dimensions but need not be square [27].

$$A = \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix} \qquad (11)$$

$$Q = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \qquad (12)$$

Q is the identity matrix with order of A, as mention in expression (11, 12). The set of Linear Matrix Inequalities (LMI's) are dependent on the eigenvalues of the Laplacian matrix. LYAP continuous-time Lyapunov's equations.

X = LYAP (A, Q) solves the Lyapunov's matrix equation (13)

A*X+X*A'+Q=0 (14)

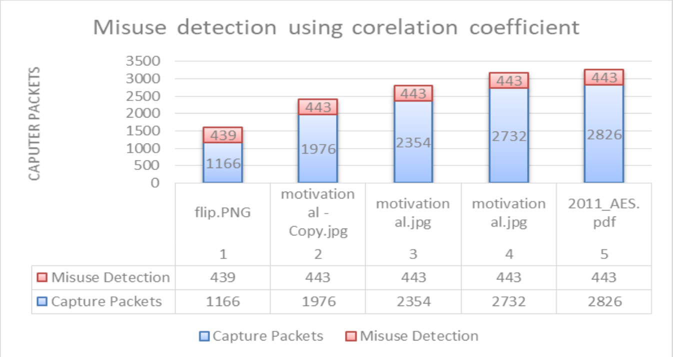
X=LYAP(A,B,C) solve the Sylvester equation (15) A*X+X*B+C=0

(16) In short, this method is use to decides whether the system is stable (without attack) or not (under attack). If Eigen values of Laplacian matrix is positive finite then system is stable, or if Eigen values of system is not positive definite then system is not stable.

Attack Frequency: let,N_f(T1, T2) denote the number of attacks taking place over (T1, T2). Here T1 and T2 are denote time [1], [2].

4. Result Analysis

In above section, detection of dos attack is done by correlation of coeffient. Below Fig.3 Shows misuse detection with respect to capture packet. As shown in below figure 4, Agent 1, Agent 2, Agent 3, Agent 4 and Agent 5 select file for communication. While selection of file, traffic is generated. This Misuse is calculated by Correlation of coeffient as shown in expression (7).



	flip.PNG 1	motivational - Copy.jpg 2	motivational.jpg 3	motivational.jpg 4	2011_AES.pdf 5
□ Misuse Detection	439	443	443	443	443
□ Capture Packets	1166	1976	2354	2732	2826

Fig 3. Detection of Misuse using Correlation of Coefficient

By comparing graph of Misuse detection using Correlation of coeffient and Threshold adaptive algorithm, for i.e while selection of flip.png detection of misuse is carry on mean value that is 233 packet(shown in Table 1 and Fig 4) where as for same file using correlation of coeffient misuse is detected by corelation coeffient value that is 668 which is calculated by Expression 7.

Table 1.Mean, Median, Max value using Adaptive Threshold Algorithm

Agent Name	Selected File	Mean	Median	Max
1	flip.PNG	233.2	583	1151
2	motivational - Copy.jpg	395.2	988	1961
3	motivational.jpg	470.8	1177	2339
4	motivational.jpg	546.4	1366	2717
5	2011_AES.pdf	1087.2	2718	5421

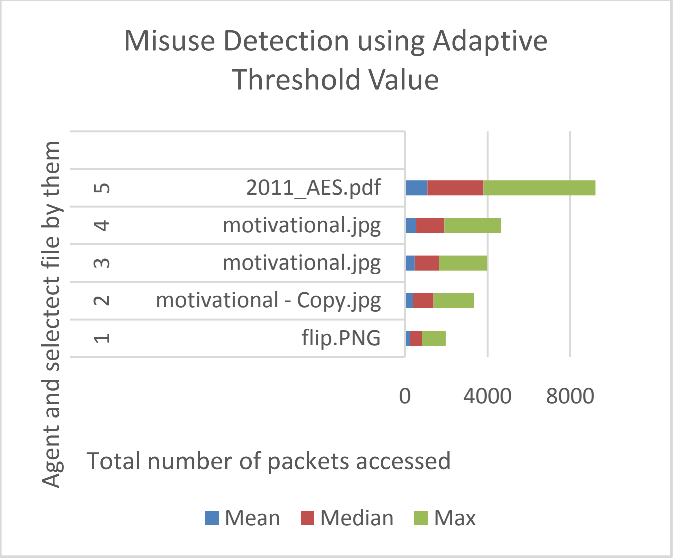


Fig 4. Detection of misuse using Adaptive Threshold.

The following Fig 5. Shows time analysis for detection of DoS attack. By comparing both result, time required for detection of DoS attack using adaptive threshold is less than correlation coefficient.algorithm.

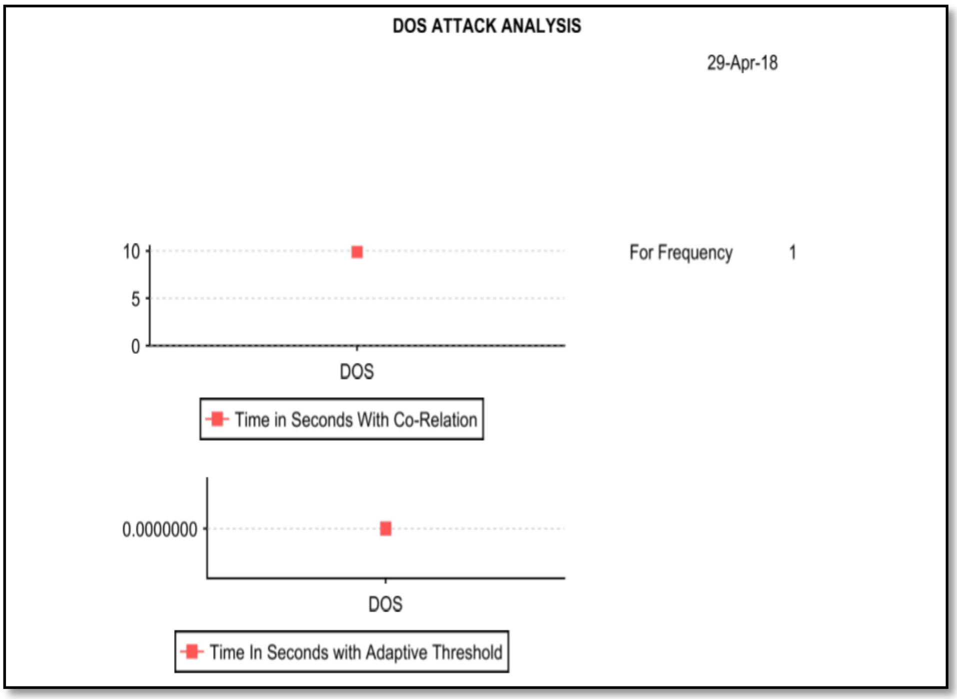
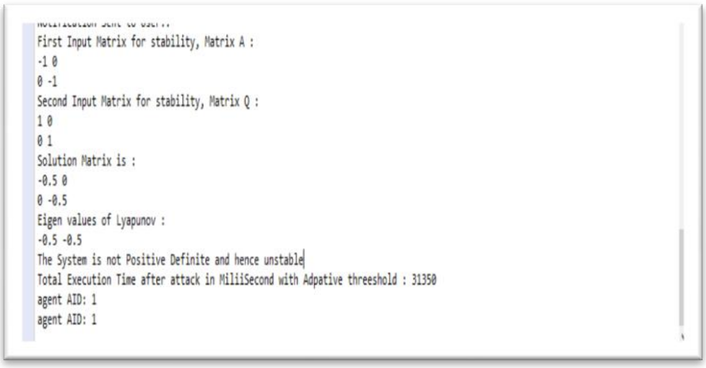


Fig 5. Time anlysis for DoS attack

Now,following result discuss regarding stability analysis. The output of Markov process is agent state prediction, which is either active or not. If current agent is active then it returns 1, or if agent is inactive then it returns -1.This is input (1,-1) for the stability calculation. By solving the Lyapunov's matrix equation X = LYAP (A, Q) as mention in expression (13), If Eigen value of Lyapunov are not positive definite it means system is unstable. In Fig 6, Eigen values are negative

(-0.5,-0.5), Hence System is unstable due to strategic attack.



```
First Input Matrix for stability, Matrix A :
-1 0
0 -1
Second Input Matrix for stability, Matrix Q :
1 0
0 1
Solution Matrix is :
-0.5 0
0 -0.5
Eigen values of Lyapunov :
-0.5 -0.5
The System is not Positive Definite and hence unstable
Total Execution Time after attack in MiliiSecond with Adpative threeshold : 31350
agent AID: 1
agent AID: 1
```

Fig 6. Stability Analysis using Lyapunov's method

The following Fig.7 shows attack frequency. As attack frequency is nothing but total number of attack over system. When Agent 1 select flip.png file, it generate traffic and misuse is detected so attack frequency become 1. Likewise Agent 2, Agent 3, Agent 4, Agent 5 behave maliciously. Hence, there are total 5 DOS attack by Agent 1,Agent 2,Agent 3, Agent 4, Agent 5.

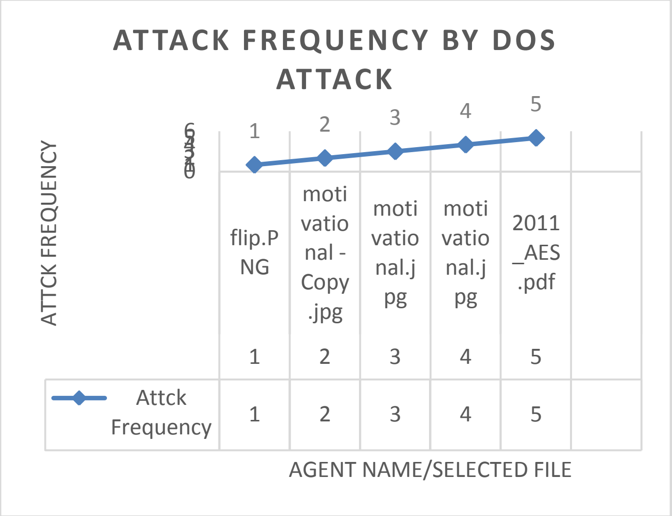


Fig 7. Attack Frequency

IV. CONCLUSION

This paper studies attack detection strategies under MAS. This paper address major two type of attack named as DOS and MIMA under MAS. Detection of DOS attack is basis on correlation of coefficient algorithm and detection of MIMA is basis on fault detection algorithm. Detection of malicious behaviour of agent is done in very less time using adaptive threshold algorithm. Finally, stability analysis of MAS is done and malicious agent is block under MAS.

REFERENCES

[1]. Supriya More ,Sharmila Gaikwad,A Study of Consensus Problem in Multiagent System, International Conference On Emanations in Modern Technology and Engineering (ICEMTE-2017,International Journal on Recent & Innovation Trends in computing & communication (IJRITCC),volume:5,Issue:3,ISSN:2321-8169,March 2017.

[2]. Zhi Feng, Distributed Secure Coordinated Control for Multi agent Systems under Strategic Attack,IEEE, 2168-2267, 2016

[3]. G. J. Solanke, P. R. Chandre, Security to Multi-agent in IDS,International Journal of Science Engineering and Technology Research (IJSETR), Vol. 3, Issue 10, October 2014.

[4]. Bordini R.H., Dastani M., Winikoff M., Current Issues in Multi-Agent Systems Development,Engineering Societies in the Agents World VII: 7th International Workshop, ESAW 2006 Dublin, Ireland, September 6-8, 2006 Revised Selected and Invited Papers ,pp.38-61,2006

[5]. Hamdane Mohamed, El-Kamel,Lezzar Fouzi,Boufenar Chaouki Mili Seif Eddine, Implementation of Multiagent System to Control adaptability in workflow environment, PDF Available online on https://www.cs.umd.edu/~jkatz/papers/thesis.pdf

[6]. Jean Tajer, Mo Adda and Benjamin Aziz, Detection of flooding attacks on mobile agents using sketch technique and divergence measures, International journal of engineering sciences & research technology, ISSN: 2277-9655, August, 2017.

[7]. Karthik Pai B.H., Nagesh H.R., Abhijit Bhat, Detection and Performance Evaluation of DoS/DDoS Attacks using SYN Flooding

Attacks, International Journal of Computer Applications, ICICT, 2014.

[8]. F. Pasqualetti, F. Dorfler, and F. Bullo, Attack detection and identification in cyber-physical systems, IEEE Trans. Autom. Control, vol. 58, no. 11, pp. 2715–2729, Nov. 2013.

[9]. Dina Shehada M. Jamal Zemerly, Chan Yeob Yeun, A framework for comparison of trust models for multi agent systems, Information and Communication Technology Research (ICTRC), 2015.

[10]. Prof. Krishnalal G. Jisha Babu, A Secure Data Transmission For Multiagent System Using Digital Signature, International Journal of Engineering Research & Technology (IJERT),Vol. 2 Issue 8, August 2013.

[11]. Esther M. Amullen, Sachin Shetty, and Lee H. Keel ,Model-based resilient control for a multi-agent system against Denial of Service attacks,World Automation congress, 2016.

[12]. Z.A. Baig, K. Salah, Multi-Agent pattern recognition mechanism for detecting distributed denial of service attacks, IET Information Security, Vol 4,Issue 4, December 2010.

[13]. V.Priyadharshini, Dr. K. Kuppusamy ,Prevention of DDOS Attacks using New Cracking Algorithm, International Journal of Engineering Research and Applications, ISSN: 2248-9622, Vol. 2, Issue 3, pp.2263-2267, May-Jun 2012.

[14]. Yonghe Guo, Chee-Wooi Ten, Shiyan Hu and Wayne W. Weaver,Modeling distributed denial of service attack in advanced metering infrastructures, Innovative Smart Grid Technologies Conference (ISGT), IEEE Power & Energy Society, 2015.

[15]. Tim Geissler, Olaf Kroll-Peters, Applying Security Standards to Multi Agent Systems, Available online onhttp://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.94.9664.

[16]. Zhongmin Wang, Xinsheng Wang, DDoS Attack Detection Algorithm Based on the Correlation of IP Address Analysis, International Conference on Electrical and Control Engineering (ICECE),IEEE,2011.

[17]. Prof. Dr. S. S Chorage, Somwanshi V. A., High Speed AES Algorithm to Detect Fault Injection Attacks and Implementation using FPGA,Global Journals Inc. (USA), Vol.17 Issue 2 Version 1.0 , 2017

[18]. Wathiq Laftah Al-Yaseen, Zulaiha Ali Othman, and Mohd Zakree Ahmad Nazri, Real-Time Intrusion Detection System Using Multiagent System,International journal of Computer Science, February 2016.

[19]. A.Annie Bibiana, DR. R. S. Shaji, J. P. Jayan, An Optimized Secured Service selection under Mobile Adhoc Networks, International Conference on Control, Instrumentation, Communication and Computational Technologies ,IEEE,2014

[20]. Abhinav S. Raut, Kavita R. Singh, Anomaly Based Intrusion Detection-A Review,ACEEE, Int. J. on Network Security, Vol. 5, 2014.

[21]. Esther M. Amullen, Sachin Shetty, and Lee H. Keel, Secured Formation Control for Multi-agent Systems under DoS Attacks,Technologies for Homeland Security (HST), IEEE Symposium, 2016.

[22]. Markov Process, PDF available online onhttps://people.math.osu.edu/husen.1/teaching/571/markov_1.pdf

[23]. An Introduction to Markov Decision Process, PDF available online onhttps://www.cs.rice.edu/~vardi/dag01/givan1.pdf

[24]. Faizal M. A., Mohd Zaki M., Shahrin S., Threshold Verification Technique for Network Intrusion Detection System, International Journal of Computer Science and Information Security,Vol. 2, No. 1,2009.

[25]. Aqeel sahi, david lai, yan li, mohammed diykh, An Efficient DDoS TCP Flood Attack Detection and Prevention System in a Cloud Environment, IEEEACCESS, Vol.5, 2017.

[26]. Specification and design NIDSMAM, PDF available online on http://shodhganga.inflibnet.ac.in/bitstream/10603/98261/13/13_chapter5.pdf

[27]. Lyap, documentation file available online onhttps://in.mathworks.com/help/control/ref/lyap.html

Supriya More." Detection of Malicious Behaviour of Agent Using Attack Detection Strategies under Multiagent System.” International Journal Of Modern Engineering Research (IJMER), vol. 08, no. 05, 2018, pp. 33–41.