Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

Efficient Detection of Location Based Routing Attack by Routing Attack Mitigation in Mobile Agent Systems

Dr.C.Shanmuganathan[1],Dr.K.Boopalan[2]
[1]Assistant Professor, Department of CSE,SRM Institute of Science and Technology, Ramapuram, Chennai,drcsnathan@gmail.com
[2]Associate Professor,Annamacharya Institute of Technology and Sciences, Rajampet,erbookumar@gmail.com

Abstract

New advancements are required to confront new situations because of the quick spread of the Internet. Recent years, PC frameworks have effectively developed from unified solid computing devices supporting static applications, into client-server situations that permit complex types of distributed systems for computing. The present work has been focused on finding out the network attacks happened in mobile agent systems. The proposed work is to detect the location based routing attack by Routing Attack Mitigation Algorithm which is one of the variant of classification based data mining concept. The parameters such as throughput, packet delivery, packet loss and end-to-end delay has been analyzed for evaluation using network simulator. The outcome of all the performance evaluation parameters has been depicted to improve the efficiency of the network.

Keywords: Location based routing, mitigation attacks, network performance, mobile agent system, intrusion detection, data mining

1. Introduction

The Mobile Agent Systems (MAS) depends on the presumption that works in an open world. The organized condition where an agent is working is open and without limits; it is dynamic in nature from the point of view of system topologies, specialized agent capacities and operator areas; and the arranged condition is questionable, that is, a similar operator that gave a response to a prior solicitation may not be accessible when called upon more than once.

In the MAS there is likewise a support that regularly there will be some level of administration or useful replication so that one agent could come up short, one or numerous different specialized agents and specialized agent organizations can be found to substitute for the inefficient agent. MAS framework must be space autonomous and a reusable substratum on which MAS frameworks, administrations, and parts live, convey, communicate and interoperate; the foundation should bolster specialized agents and encourage their social collaborations with one another, as opposed to force itself.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

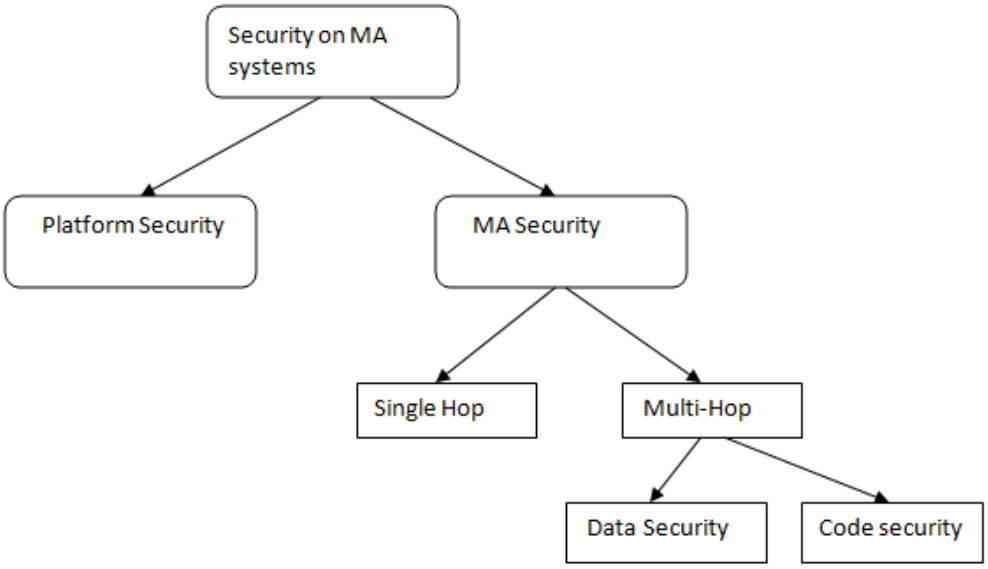

Figure 1 Mobile Agent System Classification

Figure 1 discussed on the classification on mobile agent security systems[Geetha et al.2015[1]). The basic classification is divided into platform security and Mobile agent security. The MA security is further classified in to single hop and multi hop environment. The main objective is to establish the methods for data security and code security to attain efficient mobile agent security.

2. Related Works

In this section various review works have been discussed related to mobile agent security. Our focus shows the existing works and their issues involved in making the network vulnerable.

Weijin Jiang *et al.* 2019 [2] analyzed the reasons for security issues in mobile agents .The authors also focused on the review of the issue of dynamic administration of abstract trust in mobile agent framework under the target trust the management structure of SPKI-based portable agent framework. The trust necessity of the substance (host or portable operator) in the versatile agent framework is examined, and an abstract trust dynamic management model comprising for the most part of three trust segments is proposed. However, the trust model followed a predefined model where the trust prediction constraints are slightly easier compared with other techniques.

Cheng Song *et al.* 2019 [3] investigated on the problem of circle formation in mobile gent systems. The author proposed distributed control laws for reducing the interaction range between the clusters. Moreover the radius of the circle has a significance factor in plane deployment. However, the assumptions are not followed practically in real time scenarios.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

Chengcheng Zhao et al. 2018 [4] have developed a solution for detection of malicious attacks using consensus detectors with mobility. The authors also planned another and straightforward update standard called normal emphasis to compel the conditions of assault hubs. Through partitioning attacks into Attack-II (without assaults in the neighborhood) and Attack-I (with attacks in neighborhood), they proposed two attacks identification functions, SDA and MDA. SDA uses two-hop data to ensure that Attack-II abusing the update rule in MRCA will be identified. However, these methods may not suit in all kinds of networks.

Ji-Hwan Son et al. 2015[5] discussed the integration of mobile agents with Web Services allows software adaptation to deal with a vibrant setting, automated system configuration, and changes in application requirements that are common in the ever-changing technology of today. A lightweight and effective composition of Web services based on mobile agents in accordance with the principles of Representative State Transfer (REST) for agent development, migration and control.

Muhammad Usman et al. 2015 [6] proposed the scheme that utilizes basic, yet for all intents and purposes compelling measurable systems alongside the fuzzy logic to identify cross-layer abnormalities. It additionally offers the office to transmit mobile agents after thought of the correspondence link-state. The proposed plan is actualized on a testbed and results demonstrate its capacity to recognize cross-layer peculiarities with high exactness and furthermore its capacity to diminish the energy consumption brought about by the portable agent transmissions in the poor correspondence interface state circumstances. However it does not incorporates the role-based access control mechanisms for the application software.

BurakÇakmak*et al.* 2016 [7] have been discussed on the localization of mobile networks in cooperative manner. A message passing algorithm is implemented based on the mean field message passing approach. The mobile agents were tracked using a concept of distributed belief propagation. However, the results have been discussed only on a predefined Gaussian belief approximation.

A novel system that monitors the search progress of agents with a single node to prevent duplicative searching and shows the efficacy of the system using computer simulations (Shiraki& Sugawara 2017)[8].

Florian Meyer *et al*. 2016 [10] proposed a Bayesian system and strategy for circulated consecutive localization of helpful agents and non-cooperative objects in versatile mobile systems, in view of repetitive estimations among operators and objects and between various agents. The authors work provided a reliable blend of helpful self-localization (CS) and dispersed object tracking (DT) for different portable mobile or static agents and objects only for known number of objects and agents.

Xing Liu *et al.* 2016 [11] investigated the issue of transmission vitality in the MCC condition. In light of the Lyapunov enhancement structure, a T2S2 calculation is introduced, where the tradeoff between energy proficiency and delay for multi-channel wireless networks is accomplished .However some of issues have not been focused like data transmission, local

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

execution, cloud execution, and establishment of structural properties into account to minimize energy consumption on mobile agents.

In the network executing a job in the target hosts, agents with distinct functionalities roam. This enables to significantly reduce network traffic. Mobile agents ' vulnerability to a multitude of attacks is a prominent problem for more extensive application of this technology (Budhkar et al. 2012)[12].

The survey shows that the real time security tools and proposals have been developed to improve the security of the mobile agents recent time. Network Performance reduces because of the increase in number of promiscuous users in network. Resource-sharing and robustness is less in the network and Theperformance analysis was done only for single temporal agent.

3. Methodology

The area data of the versatile nodes of the MAS is utilized as the way to perform directing attack identification. The versatile nodes have the property of portability which has no restriction and confinement toward them. As the versatile nodes are proceeding onward its very own in various ways, the topology is liable to change in the whole division. As a rule the portable nodes perform route disclosure and dependent on the aftereffect of the route revelation, a solitary way is chosen. The vindictive node sends mismatch data to be chosen in the directing procedure. The source node would surmise the target so as to diminish the vitality misfortune in information transmission. In the event that the neighbor chose is practically out of the scope or out of the transmission extend then the source node spends higher vitality to perform information transmission that moves to the neighbor[13][14].

In reverse case, if the vindictive node is altogether out of the transmission scope of the source node, however it would have higher radio sign with higher transmission run which gets the solicitation from the source node and could straightforwardly impart to the neighbor of the sink node. At the point when the node has been chosen as the forwarder, it would either perform to identify stealthily attack or it would perform sink opening attack to destroy the principal neighbor of the sink area node. Such noxious node is distinguished by approximating the area of the vindictive node. Every node would move specifically by a route and moves in a threshold speed, as there would be an unequivocal change in the area of the versatile node[15][16]. The source node would keep up the area data of the neighbors and the route being pursued. In view of the data the area estimate is performed to recognize the nearness of malicious attack[17].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

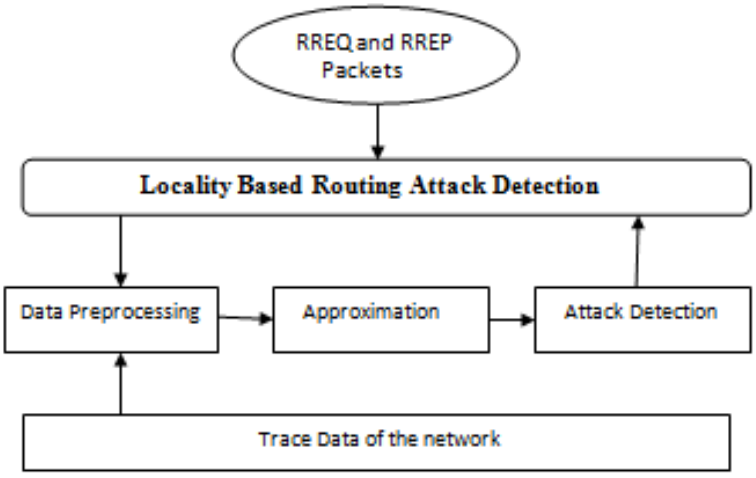

Figure 2 Locality Based Routing Attack Detection

In the Data preprocessing stage, the system follow is perused and it distinguishes the rundown of follows that have a place with the course and the neighbor. The strategy distinguishes from the follows the rundown of areas where the node was situated in the past transmission. Distinguished area data is utilized to perform relief as shown in Figure 2.

In Location approximation[18], the area subtleties got from preprocessing stage utilizes the speed data to process the conceivable area. Essentially the neighbor rundown of different nodes is confirmed for the nearness of the client node in their rundown. The routing attack is identified utilizing the approximated values based on the location.

The source node contains various neighbors and just through the neighbors the node arrives at its goal. In the first place, the strategy creates a control message and communicates the system. On accepting the solicitation, the neighbor sends the answer. At the point when the source node gets the answer it separates the different data from the answer and adds to the neighbor table. The neighbor sends answer with different data like area, vitality and speed. Such data is recovered and put away in the neighbor table. This data is utilized later to perform routing attack location. The following algorithm is used to examine for identifying neighbor revelation to gather the data about neighbors and attack mitigation as shown in Table 1.

Table 1 Routing Attack Mitigation Algorithm

Input: Route Table Rt, Network Trace NeT, Packet P.Neighbor Table Nt.
Output: Null
Step 1: Read Neighbor Table Nt.
Step 2: Read Packet P.
Step 3: Identify neighbors by neighbor discovery.
Step 4: Perform route discovery.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

Step 5: For each route
Compute trust weight for first neighbor.
Compute Trust weight .
For each intermediate node
Compute location factor.
End
If LF>0
Else
Remove route from table
End.
End
Step 6: Choose most trusted route
Step 7: Forward data packet
Step 8: Stop.

4. Implementation and Results

In this section, the results of Locality Based Routing Attack Detection have been discussed. The NS2 simulator is used where 100 nodes have been created with 800×800 grid with nominal regulatory parameters.

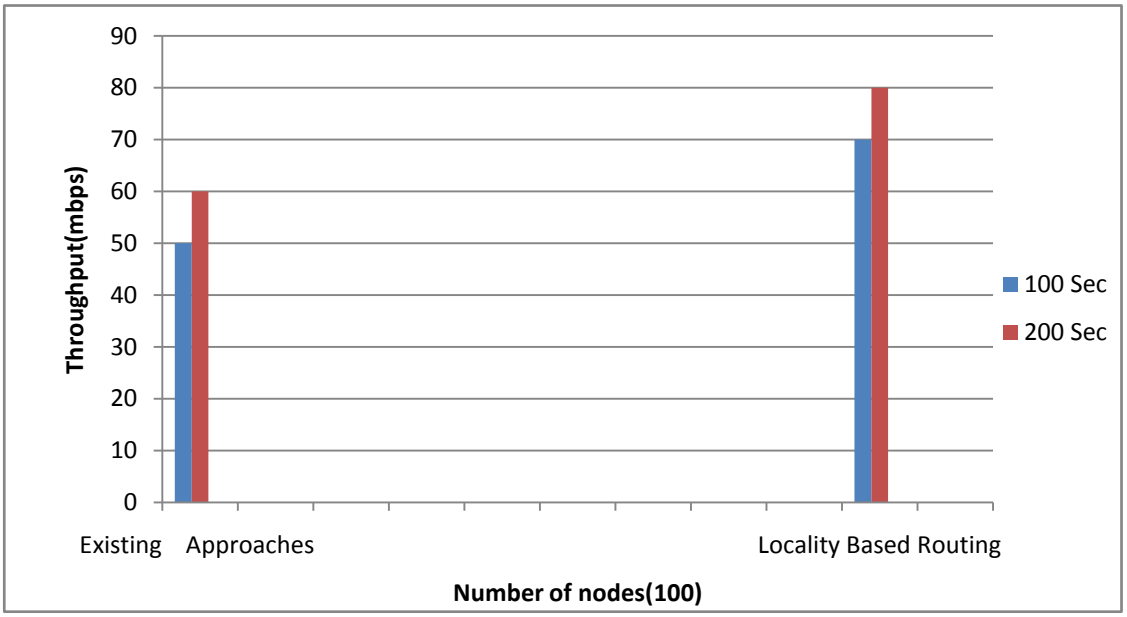

Figure 3 Throughput for Locality Based Routing Attack Detection

In Figure 3, the throughput is increased by 20% compared with existing approach. The attack detection mechanism is implemented and the results are compared with before attack, after attack and prevention which is followed in further network parameter discussion.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

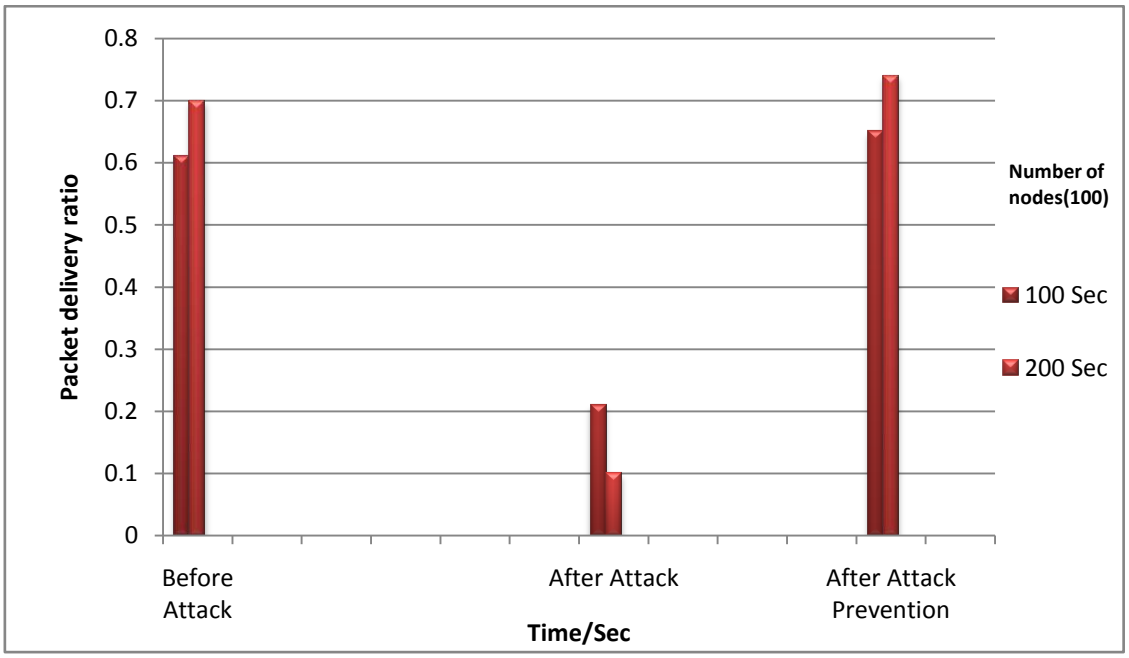

Figure 4 Packet delivery ratio for Locality Based Routing Attack Detection

The packet delivery ratio has been retained by 70% through implementation of location based detection for proving the mobile agent security. The results are shown in Figure 4.

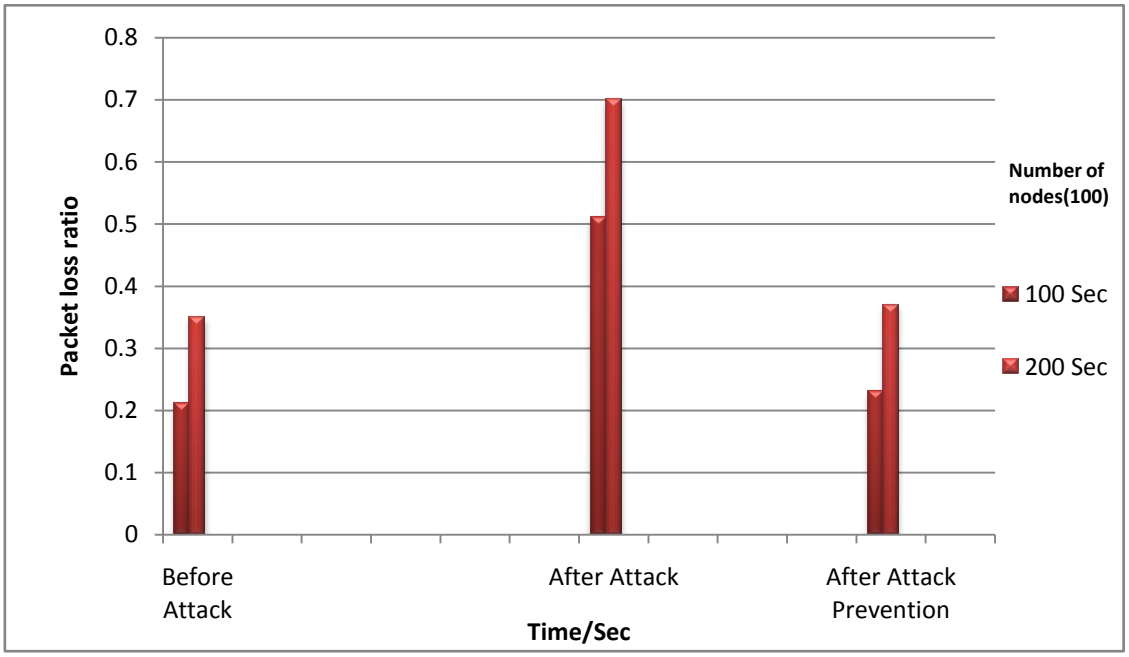

Figure 5 Packet loss ratio for Locality Based Routing Attack Detection

The packet loss ratio has been reduced by 10 % through the implementation of locality based detection. The results have been depicted in Figure 5.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 5, 2021, Pages. 673-681
Received 15 April 2021; Accepted 05 May 2021.

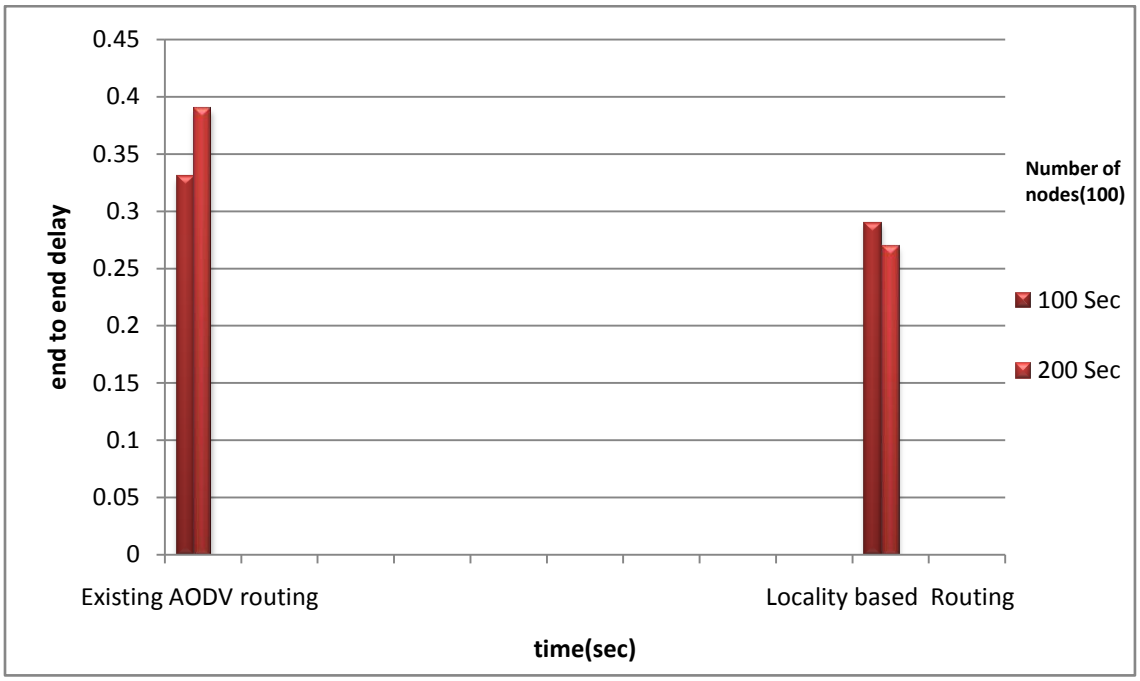

Figure 6 End to End delay for Locality Based Routing Attack Detection

The attack detection is confirmed by analyses of delay in data transmission. Hence the end to end delay has been depicted in Figure 6 and implicates a decrease of 15%.

5. Conclusion

The proposed Locality Based Routing Attack Detection route mitigation algorithm has been implemented and analyzed with respect to some of the network performance parameters such as network overhead, throughput, packet loss, packet delivery ratio and end to end delay.The analysis of the approaches concludes that there is a 15 % increase in efficient data communication between the mobile nodes based on the scaling factors of network performance parameters.

References

[1]Geetha , G and Jayakumar, C 2015, 'Implementation of Trust and Reputation Managementfor Free-Roaming Mobile Agent Security', IEEE SYSTEMS JOURNAL, VOL. 9, NO. 2, pp 556-566.

[2] Weijin Jiang, Yang Wang, Yirong Jiang, Jiahui Chen, YuhuiXu, Lina Tan, 2019, Research on Mobile Internet Mobile Agent System Dynamic Trust Model for Cloud Computing,IEEE China Communications , Volume: 16 , Issue: 7,pp 174-194.

[3] Cheng Song , Lu Liu , and ShengyuanXu , 2019 , Circle Formation Control of Mobile Agents With Limited Interaction Range, IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 64, NO. 5, pp 2115-2121

[4]. Chengcheng Zhao,JianpingHe andJiming Chen, 2018, Resilient Consensus with Mobile Detectors Against Malicious Attacks, IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS, VOL. 4, NO. 1, pp 60-69.
[5]. Ji-Hwan Son, and Hyo-Sung Ahn, 2015, 'Formation Coordination for the Propagation of a Group of Mobile Agents via Self-Mobile Localization', IEEE SYSTEMS JOURNAL, VOL. 9, NO. 4, pp 1285-1298.
[6] Muhammad Usman, VallipuramMuthukkumarasamy, and Xin-Wen Wu 2015, 'Mobile Agent-Based Cross-Layer Anomaly Detection in Smart Home Sensor Networks Using Fuzzy Logic, IEEE Transactions on Consumer Electronics, Vol. 61, No. 2,pp 197-205
[7] BurakÇakmak, Daniel N. Urup, Florian Meyer, Troels Pedersen, Bernard H. Fleury and Franz Hlawatsch, 2016 , 'Cooperative Localization for Mobile Networks: A Distributed Belief Propagation – Mean Field Message Passing Algorithm', IEEE SIGNAL PROCESSING LETTERS, VOL. 23, NO. 6,pp 828-832.
[8]YumetoShiraki , Shinji Sugawara, 2017 , 'Efficient content search method using network mobile agents with sharing searching progress' , IEEE International Conference on Consumer Electronics - Taiwan (ICCE-TW), pp 45-52.
[10] Florian Meyer, OndrejHlinka, HenkWymeersch, Erwin Riegler and Franz Hlawatsch, 2016, 'Distributed Localization and Tracking of Mobile Networks Including Noncooperative Objects', IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORKS, VOL. 2, NO. 1, pp 57-71.
[11] Xing Liu, Chaowei Yuan, Zhen Yang, and ZengpingZhang , 2016 , 'Mobile-agent-based energy-efficient scheduling with dynamic channel acquisition in mobile cloud computing', Journal of Systems Engineering and Electronics, Vol. 27, No. 3,pp 712-720.
[12]ShilpaBudhkar, Anshita Mishra, Ferdous A. Barbhuiya, Sukumar Nandi "Security in Mobile Agent Systems with Locator Mechanism" first Int‟l Conf. on Recent Advances in Information Technology | RAIT-2012 | Dept. of Computer Science and Engineering Indian Institute of Technology Guwahati, India, 781039.
[13] Shanmuganathan C, Raviraj P, Performance analysis of secure group key mechanism in Mobile Ad hoc networks, International Journal of Engineering and Technology(UAE), 2018, 7 (4.10 Special Issue 10), pp. 344–348.
[14] Shanmuganathan C, Raviraj P, A comparative analysis of demand assignment multiple access protocols for wireless ATM networks, Communications in Computer and Information Science, 2011, 204 CCIS, pp. 523–533.
[15] K.Boopalan, A Rajesh, "Traffic Analysis Based On Web User Behavior" International journal for applied engineering research, ISSN 0973-4562 Volume 10, Number 3 (2015) pp. 8287-8296.
[16] K.Boopalan, C.Nalini ,A Rajesh "Mining Opinions About Traffic Status Using Twitter Messages" International Journal of Civil Engineering and Technology(IJCIET) Vol 8, Issue 2,February (2017) ,pp 218 – 225 ISSN : 0976 – 6316.
[17] K.Boopalan, A Rajesh, "Traffic Prediction and forecasting using classification of twitter streem analysis" International journal of control theory and Applications" ISSN:0974 – 5572 Vol 9 , Number 28 (2016) pp. 319 -324.
[18]Magesh Kumar, S., Sathish Kumar, P.J., Parthipan, V. Enhanced cloud computing techniques with sophisticated network security,International Journal of Pharmacy and Technology, 2016, 8(4), pp. 23690–23701