ATLANTIS PRESS

Advances in Engineering Research (AER), volume 142

International Conference for Phoenixes on Emerging Current Trends in Engineering and Management (PECTEAM 2018)

Resilience Secured Architecture by Deploying Overlay Network in Cyber Physical Systems

[1]S.Prayla Shyry, [2]S.L Jany Shabu, [3] J.Refonaa,[4] Steffi Sterlin

[1,2,3,4] Assistant Professor, Faculty of Computing,

Sathyabama University, Chennai, India,

suja200165@gmail.com

***Abstract*—Communication networks in Cyber Physical Systems exchange the data between different devices or participants within a system. In those networks, nodes are not only used for transmitting and receiving the data, but also for deciding the path of data flow. As the nodes must store the routing table and update the same periodically to transmit the data, the overall data forwarding efficiency of these nodes decrease. Hence in the recent years, the paradigm has shifted to Overlay Networks that employ Source Routing or Selfish Routing in Cyber Physical Systems. Also Cyber Physical Systems that employs overlay network, Selfish Overlay Routing yields close to optimal average latency which is much lower than that of network level routing. However Selfish Routing has the tendency to select the routes greedily to optimize their own performance which results in serious performance degradation of the entire network due to the lack of cooperation. Hence it introduces instability in the network and increases the latency drastically. If appropriate detection of link failures is done, the performance of the network may be increased. So fuzzy logic is used to determine the probability of link failure and the link that has high probability of link failure is deliberately failed in the network. Thus the main objective of the proposed work is to develop a stabilized Cyber Physical Overlay Network (CPON)and rule based dynamic deployment of overlay nodes to provide better performance when compared to conventional unstabilized Random Deployment of Cyber Physical Overlay Network (RDCPON).**

***Index Terms*— Cyber Physical Systems, fuzzy logic, paradigm.**

I. INTRODUCTION

The existing work deploys overlay nodes randomly over the cyber physical overlay network. If a link failure occurs in a large network, more overlay nodes are deployed even in places where there is no link failure and hence leads to numerous memory consumption in Random Deployment of Cyber Physical Overlay Network. Hence effective rule based techniques are developed by fuzzy logic to decide the number of overlay nodes to be deployed only, whenever and wherever it is required.

The unbridled stabilization of Cyber Physical Overlay Network has contributed to the enormous data loss. Thus the main objective of the proposed work is to develop a stabilized Cyber Physical Overlay Network and rule based dynamic deployment of overlay nodes to provide better performance when compared to conventional unstabilized Random Deployment of Cyber Physical Overlay Network (RDCPON). Nash Equilibrium is the well known game theory approach that is used extensively for solving the instability problems of the network. Initial step of the proposed work is to attain the stabilization and to enhance the selfish routing in cyber physical overlay network performance. Taxation of edges and dual formulation techniques are adopted to decrease the latency and balance the link utilization. The performance of the selfish routing in cyber physical overlay network yields good result when used in M/M/1 queuing model. The intelligent rule based technique for stabilized Selectively Deployed Cyber Physical Overlay Network (SDCPON) results in better performance when compared to unstabilized Random Deployment of Cyber Physical Overlay Network (RDCPON). Hence this work serves as a concrete step in disproving the theoretically worst case fears about Source or Selfish Routing in Cyber Physical Overlay Network.

Objectives

- To stabilize the Random Deployed Cyber Physical Overlay Network (RDCPON) using Nash Equilibrium
- To further improve the performance of RDCPON by adopting taxation of edges and dual formulation for reducing the latency and balancing the link utilization.
- To develop intelligent rule based Selectively Deployed Cyber Physical Overlay Network (SDCPON) and to study its characteristics.
- To compare the performance of the RDCPON and SDCPON.

II. LITERATURE REVIEW

Matthias M. Herterich et al. 2015 presents an important step for understanding the impact of CPSs on industrial services. CPS transforms the service business in manufacturing and offer new opportunities for business innovation in the servitized manufacturing industry. Based on many explorative case studies with manufacturers, service organizations and equipment, they explored how CPSs transform the service business in the equipment manufacturing industry. The authors identified service affordances and investigate the impact of CPSs on various stakeholders in the industrial service ecosystem. For practitioners**,** their research provides valuable insights on the affordances of CPSs for the service business and how to exploit the new technological capabilities most effectively. *For scholars*, the work of Matthias provides

the first explorative insights into challenges and affordances related with leveraging CPSs for industrial service offerings, and serves as a foundation for further research on CPSs and the industrial service business.

Gaddadevara Matt Siddesh -Cyber-Physical Systems: A Computational Perspective CRC Press 2015 describes that CPS need to be more secure, more safe should be able to operate in real time and must be dependable. The author claim to achieve the secure CPS, security should be applied in the design phase itself rather than attempting to meet those by just using add - on security mechanisms. The researcher also identified that one – off system useful for specialized scientist and technicians to develop a contemporary infrastructure that seems to be general but a powerful system, which can be useful for majority in community.

Dr. Clifford Neuman et.al 2016 generalizes the Cyber-physical systems have additional security requirements with the addition of physical control and communication channels, real time requirements, and their common application to critical infrastructure. To achieve secure cyber-physical systems, prime step to be considered in which security to be taken into account at the very start of the design process for such systems, by enumerating the specific information flow, control, and availability requirements and ensuring that those requirements are met through all parts of the design of the system, rather than attempting to meet them only with add-on security mechanisms.

Design tools can be developed that will force developers to specify and meet such requirements. Also develop Operating System, networking, and middleware components that can separately enforce such constraints as underlying invariants within the system on which such Cyber-Physical Systems are implemented.

Lokesh. M. R et.al 2016 depicted that resilience is the property of a system to continue in its operation and provision of services in an acceptable quality even though the system is exposed to any kind of errors. A system with high resiliency should be able to detect any kind of failures as early as possible and should be able to self heal and also should be able to recover faster to continue to meet the demands for services. If an application is critical then high resilience comes into play (e.g. automated brake control in vehicular Cyber Physical Systems).

While designing a highly resilient CPS, a complete understanding of important failures and errors with the resilience properties of the required application, and evolution of system due to the dynamically varying nature of the operational environment.

To add resiliency to CPS, several techniques proposed artificial intelligence and danger theory based immune algorithms. Those techniques use the concepts of agents, self awareness and self healing approaches to achieve resiliency and make the system fault tolerant.

To avoid security challenges there are different solutions like context aware security framework for CPS that uses dynamic adaptability to the physical environment by the assistance of context coupling, use of distributed real-time software, use of competitive and cooperative resource management, using virtual test beds, use of highly confidential software to avoid security issues, integrating simulation and emulation platforms for security purposes, experimenting with different architectures to find the best suited architecture based on requirement of application, use of sandboxing controllers for Cyber - Physical Systems

Amit Kumar tyagi 2016 has challenged that no existing tools are well suited for CPS design.Since sensing data are no longer owned by local devices, security and privacy issues are become more critical in CPS. also he investigated that the country is protected from internal attacks but not from External attacks. Now we are in a new era where providing secure and powerful cyber infrastructure will help us to protect many of lives and will provide different experiences to human beings that no one has provided before.

III. PROPOSED METHODOLOGIES

Following are the proposed methodologies and figure 1 shows the workflow diagram of Cyber Physical Overlay Network

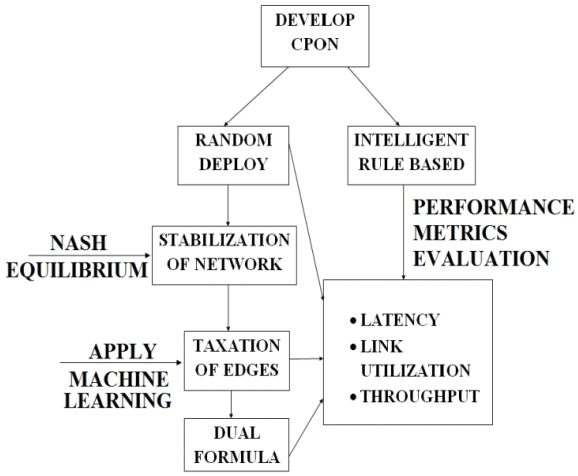

Fig. 1. Workflow diagram of Cyber Physical Overlay Networks

A. *Detection of link failures and stabilization of network*

Though extensive research has been carried out in improving the performance of overlay networks, intelligent identification of the exact location of link failure is still unresolved. Performance of Overlay networks can be improved if suitable detection of link failures and deployment of overlay nodes in exact locations are made.Fuzzy rules are generated with four distinct input parameters namely loss of signal, loss of synchronization, faulty interface and link capacity as they can be easily quantified. IF-THEN rules with "AND" implications is used for comparing the input membership functions for detecting the link failures.

Even though an Overlay network is the best solution for link failures, it suffers from instability problem. Nash Equilibrium is a well known game theory approach that is

used extensively for solving the instability problems. Nash Equilibrium constructs a stable network from the set of selfish nodes that may otherwise lead to inefficiency due to the lack of co-operation between the users. A flow f is at Nash Equilibrium if all the edges in the flow experience minimum delay.

B. Taxation of edges and reinforcement learning algorithm

Taxation of edges is a technique which charges each network user for the congestion caused by its presence on the edges. More precisely it means each time the user uses a route the user has to pay a tax to the upstream node. As the taxes for the edges are not stabilized and an artificial intelligence concept is adopted to stabilize the taxes, reinforcement learning algorithm uses precedent experience in optimal decision making through trial and error interactions with external environment. Also optimized strategic decisions based on past experiences in overlay networks are undertaken.

C. Dual formulation

The objective of dual formulation is to determine how much demands should be accepted and how to distribute each among the links so that total utilization of link is minimized.

D. Intelligent rule based selectively deployed cyber physical overlay network

Extensive research is carried out to deploy the overlay nodes only when and where there is a link failure. Intelligent rule based technique is proposed to deploy the overlay nodes dynamically. Overlay nodes are deployed by fuzzy logic during the link failure.

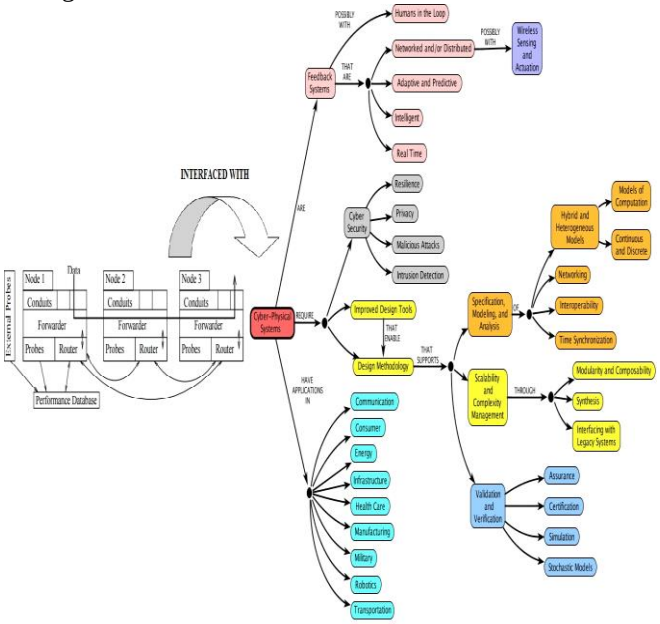

Fig. 2. General architecture of Overlay Network interfaced with Cyber Physical Systems

IV. EXPERIMENTAL RESULTS

A mesh topology is created with 100 nodes and the Ns2 parameters are shown in Table 1. NS2 is used for the simulation of network and it is the Object-oriented Tcl (OTcl) script interpreter that has a simulation event scheduler and network component object libraries, and network setup (plumbing) module libraries.

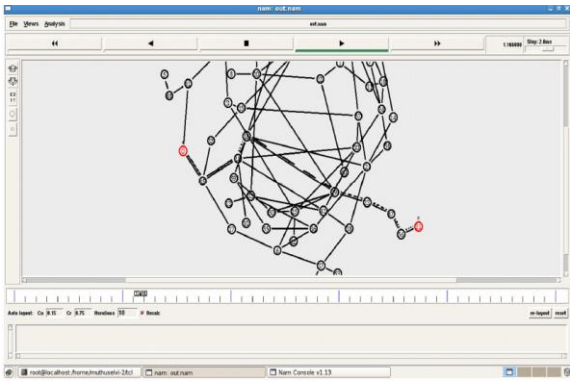

Fig. 3. Simulation graph of RDCPON for M/M/1 queuing model

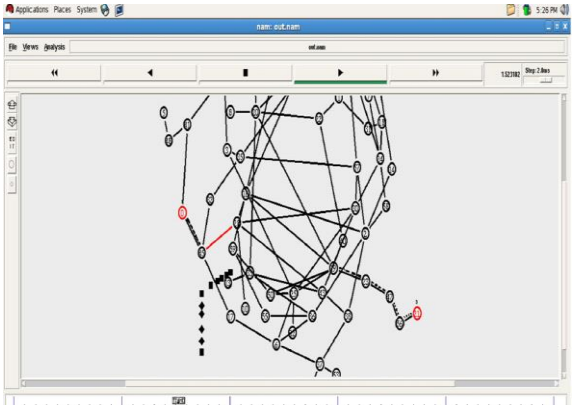

Fig. 4. Simulation graph of link failure and packet drop in RDCPON for M/M/1 queuing model

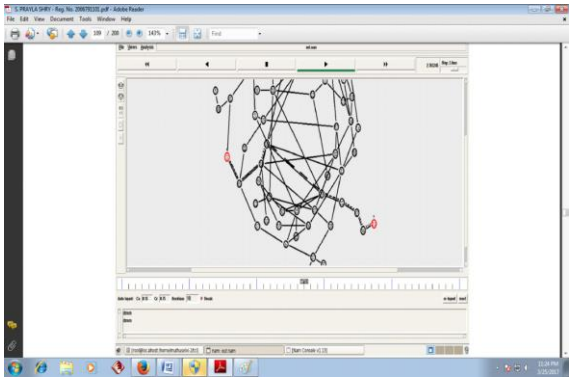

Fig.5. Simulation graph of packet transmission after path outages

It is noteworthy that the link failure is detected and recovered from path outages within 0.07 ms in Random Deployment Cyber Physical Overlay Network.

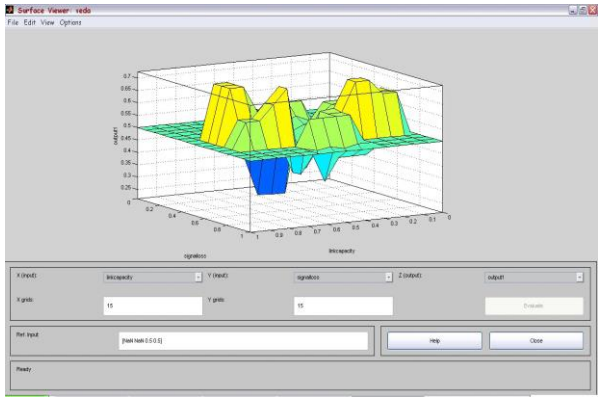

Fig. 6. Surface view of link capacity and signal loss for triangular membership function (X-axis: link capacity, Y-axis: Signal loss, Z-axis: probability of link failure)

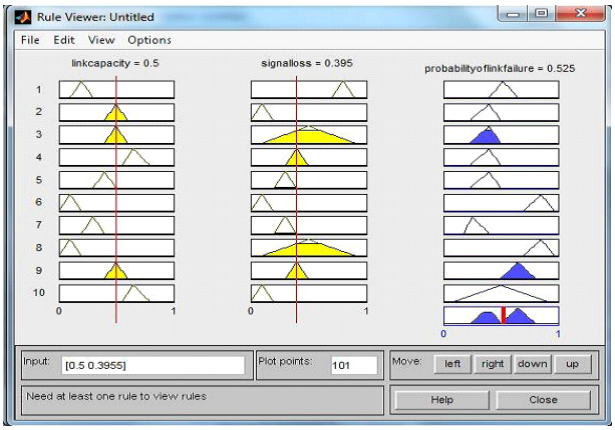

Fig. 7. Rule viewer for link capacity and signal loss for triangular membership function . It is clear from the figures that if link capacity is 0.5 kb and signal loss is 0.395 then the probability of link failure is 0.525 percentages

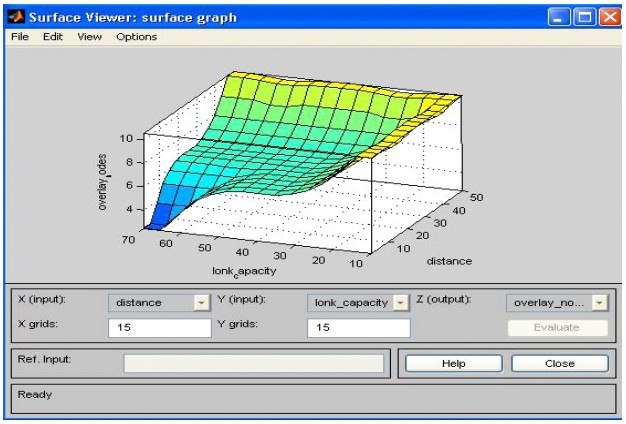

Fig. 8. Surface graph in MatLab for overlay nodes. (X-axis: distance, Y-axis: link capacity, Z-axis: No of overlay nodes)

Simulation result shows that if the distance is high and link capacity is low then more number of overlay nodes is deployed. Also for example if the distance is 15 and link capacity is also 15 then the number of overlay nodes to be deployed is 8.

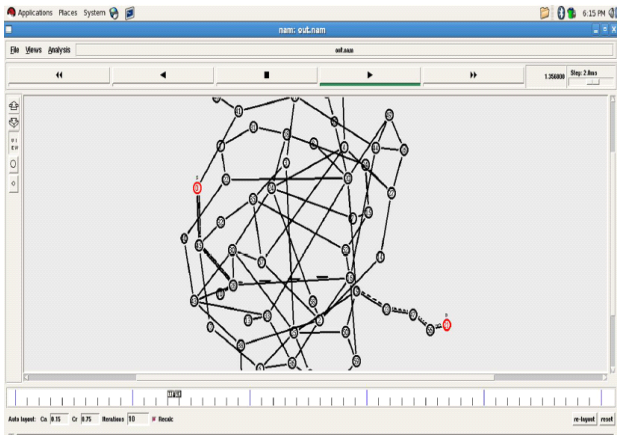

Fig. 9. Simulation graph of Selectively Deployed Cyber Physical Overlay Network

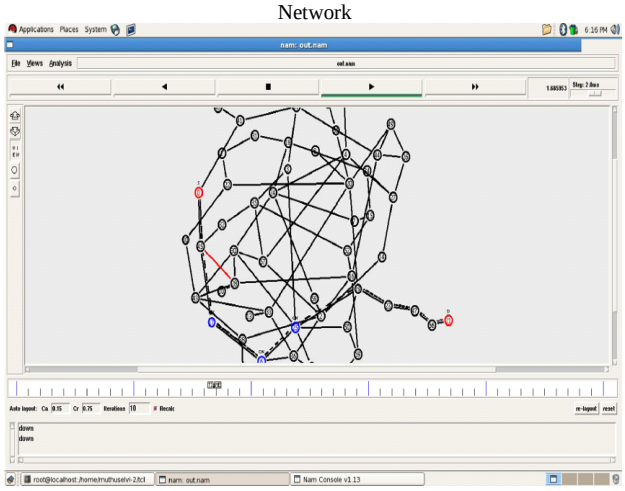

Fig.10. Free flow of packets after intelligent rule based Selectively deployed Cyber physical overlay network

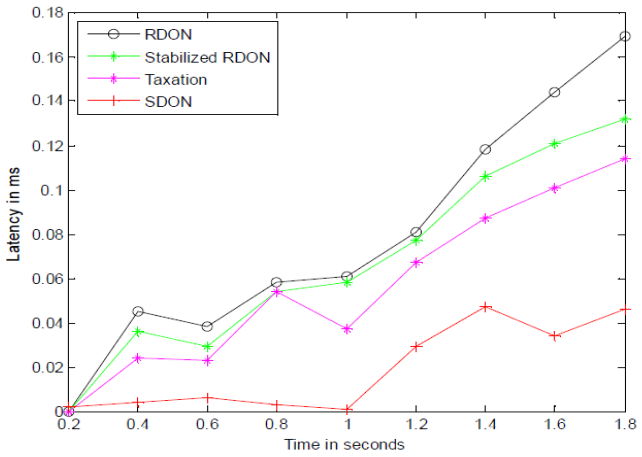

Fig. 11. Latency in Source Routing for M/M/1 queuing model

From the results, it is clear that latency is less in intelligent, dynamic deployment of overlay nodes in the network compared to the conventional unstabilized RDCPON, Stabilized RDCPON, RDCPON after adopting taxation.

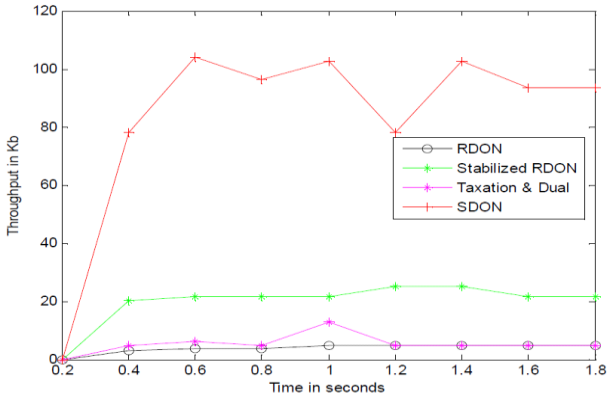

Fig.12. Throughput in Source Routing for M/M/1 queuing model

It is inferred from the results that throughput is increased in SDCPON compared to conventional techniques. When 1000 packets are transmitted, throughput in SDCPON is 102.54 kb which is much higher than 4.88 kb achieved in RDCPON for source routing in M/M/1 queuing model.

V. Conclusion

An intelligent rule based system is developed to determine the number of the overlay nodes, and the nodes are deployed dynamically only in places where there is link failure. In SDON, when 1000 packets are transmitted, the average latency is 0.0009 ms, link utilization is 0.08 Mb and throughput is 102.54 Kbps at 1ms for Source Routing in M/M/1 queuing model. When compared to conventional random deployment of overlay network, average latency is 0.06 ms, average link utilization is 0.87 Mb less in intelligent and dynamic deployment of overlay nodes in SDON.

References

[1] Roughgarden T (2002), "Selfish Routing", PhD thesis, Cornell University.

[2] Sabyasachi Roy, Himabindu Pucha, Zheng Zhang, Charlie Hu Y. and Lili Qiu (2009), "On the Placement of Infrastructure Overlay Nodes", IEEE/ACM.

[3] Salah. A. Aly and A. E. Kamal (2008), "Network coding-based protection strategies against a single link failure in optical networks",In Proc. IEEE International Conference on Computer Engineering & Systems, pp 251-256.

[4] Sebastian Kniesburges, Andreas Koutsopoulos, Christian Scheideler (2011)," Re-Chord: A Self-stabilizing Chord Overlay Network", SPAA'11, June 4–6.

[5] Shailesh Kumar, Dr. M.Siddappa (2011)," Reliable Routings in Networks with Generalized Link Failure", International Journal of Smart Sensors and Ad Hoc Networks (IJSSAN) Volume1,Issue-1, pp.76-79.

[6] Abhay Parekh (2002),"Routing on Overlay Networks", EECS Berkley University.

[7] Aditya Akella, Srinivasan Seshan, Richard Karp, Scott Shenker, Christos Papadimitriou (2002), "Selfish behavior and stability of the internet:: a game-theoretic analysis of TCP",Proceedings of the of the conference on Applications, technologies, architectures, and protocols for computer communications", SIGCOMM,' pp. 117-130.

[8] Aditya Kumar, Mishra, Anirudha Sahoo and Kanwal Rekhi (2007), "S-OSPF: A Traffic Engineering Solution for OSPF based Best Effort Networks", In Proceedings of GLOBECOM,IEEE, India, pp. 1845-1849.

[9] Ahmed Kamal E. and Aditya Ramamoorthy (2011), "Overlay Protection Against Link Failures Using Network Coding", IEEE ACM Transactions on networking, Vol.19, Issue 4, pp.1071-1084.

[10] Amit Kothari D. and Ashok Patel R (2010), "On Demand Temporary Parallel Route Recovery for Frequent Link Failure in Adhoc Networks," International Journal of Computer Applications,Vol. 11, No. 11, pp. 1–6.

[11] Jocylene Elias, Fabio Martignon , Konstantin Avrachenkov and Giovanni Neglia (2010),"Socially Aware Network Design Games", Proceedings of the 29th conference on Information communications, pp. 41-45.

[12] Junghee Han, David Watson and Faenam Jahanian (2005), "Topology Aware Overlay Networks", Proceedings on 24th Annual Joint Conference of the IEEE Computer and Communications Societies, INFOCOM, Vol. 4, pp. 2554-2565.

[13] Kyung Seob Moon, Vallipuram Muthukkumarasamy, Anne Thuy-Anh Nguyen (2006), "Reducing network latency on consistency maintenanace algorithms in distributed network games", Proceedings of the IADIS International Conference: Applied Computing, Spain, pp.137- 144.

[14] Kyung Seob Moon, Vallipuram Muthukkumarasamy, Anne Thuy-Anh Nguyen (2006),"Reducing network latency on consistency maintenanace algorithms in distributed network games", Proceedings of the IADIS International Conference: Applied Computing, Spain, pp.137- 14