LOAD OPTIMAL MPLS ROUTING FOR DENSE NETWORKS

CHOCKALINGAM.A
BALAJI.S
KARTHICK RAJAN.P

ADVISOR:DR.S.GOMATHI

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

FX Engineering College,Tirunelveli,TamilNadu, India

Abstract— **Thehomogeneous data fusion Fog Computing based intelligent directional mesh network architecture, routers, gateways and even actuators can be potentially used as end Fog nodes. The Fog nodes will extract different features from real-time state information of network nodes using trained machine learning models and make intellectual decisions to select an optimal communication path considering the constraints such as power spending and spectrum occupation. DMN (Directional Mesh Network) become more adaptive to the local environment and robust to spectrum changes. The current research is going onimproving the appraisal performance in presence of joint node and link attack.Because the generation of original infrastructures with new services and connections. That requires more frequent vulnerability assessments. In the prior work, they have the network estimation approaches on either only network or node attacks presence. They did not consider the arrangement of the node and link attack situations. In this paper going to concentrate on the joint node and link attack and to manage the minimum cost of node and link in the network to gain the networking process.**

Keywords— **Vulnerabilityassessment,HMM algorithm,link attack, Efficient transmission, Resource Allocation.**

1. INTRODUCTION

Ensuring secure and reliable applications in wireless network depends on integrity and confidentiality, correspondingly defined as the ability to keep data secret from unauthorized entities and the ability to verify that no data has been change by external sources. Nowadays, they unruly minutes are accomplishment since regular tragedies to hateful attacks that can radically teamwork the network's ability to meeting this one quality-of-service. Infrastructures in many networks such as telecommunication, transportation networks and power grid systems are highly interdependent and sensitive to both random failures anddeliberate attacks. In fact, the fiascos of a small number of nodes may lead to a complete breakup of a network system and severely disrupt the network connectivity. Real-world examples include the unplanned annihilation of fibercables by dragging anchors, malicious cyber-attack to Internet Autonomous Systems and terrorist attacks targeting infrastructures in electrical power grids and highway systems [1]. Therefore, it is essential to judge the network defence lessens to those fatal failure schemes before they happen. There have been abundant efforts on propositioning evaluation measures of the network vulnerability, as summarized. However, these events can neither be rigorously mapped to the overall network connectivity, nor reveal the set of most critical vertices and edges, thus are not suitable to assess the network weakness in terms of connectivity [2]. To facilitate the search for critical infrastructures in networks regarding network connectivity, a new assessment method has-been proposed in form of an optimization problem, so-called -vertex disruptor. The network vulnerability was measured through the least number of nodes that removal incurs a certain level of disorder in the objective network. Extensive experiments on both synthetic and real networks showed that the new assessment method outperforms the traditional ones and successfully identifies small subsets of critical nodes that failures lead to the network wide fragmentation. In addition, the flexibility in selecting the level of disruption assessing vulnerability at multiple disruption levels, providing a complete network vulnerability spectrum [3]. To solve the -vertex disruptor problem, which was shown to be an NP-hard problem, the authors proposed a pseudo-approximation algorithm that can guarantee the performance of the optimal solutions. Despite that the algorithm is of theoretical interests, it has high time complexity and is difficult to be implemented efficiently. Besides designing algorithms with performance guarantees, the -vertex disruptor

problem can be formulated using integer programming (IP) and solved for the exact solutions by branch-and-cut methods. The same approach has been applied for the critical nodes(Edges) detection problems that seek for a set of knodes (edges) that removal maximizes the disruption in the residual network [4]. Unfortunately, even for small network instances all proposed formulations become very large integer programming problems that consume excessive amount of memory and time to converge. For example, the largest reported instance with 150 nodes consists more than one million constraints. Moreover, solving those integer programming problems relied solely on the general edition of the branch-and-cut algorithm implemented in the optimization packages that are not tailored to those specific problems [5].

2. PROBLEM STATEMENT

A key-aggregate encryption scheme consists of five polynomial-time algorithms as follows. Messages can be encrypted via Encrypt by anyone who also decides what cipher text class is coupled with the plaintext message to be encrypted. The data owner can use the master-secret to generate acollection decryption key for a set of cipher text classes via Extract. The generate keys can be passed to delegates securely (via secure e-mails or secure devices) finally any user with an aggregate key can decrypt any cipher text provided [6.7].

3. Related Work

In the prior work, they have focus only on the centrality measurements. It income measuring the degree, between's and closeness centralities[1].In the prior work, they concentrate only to identify either the critical nodes or critical links[3].In other prior work, they judge the multiple attacks which happen at both links and nodes at the same time[4]The other prior work does not work well when the network connectivity is of soaring priority[6].In the other prior work, they proved that the critical node detection problem is also the NP-complete problem on trees for the total biasedpair wise connectivity metric.

Modules

- Mesh Network streaming
- Fog based spectrum sensing
- Security based Markov Processing
- Memory Allocation and Reallocation
- Network Reconstruction Module
- Performance Evaluation

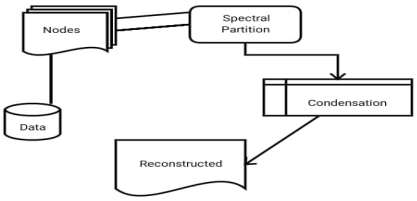

Fig. System Architecture

Proposed Technology

The multivalent system is a branch of distributed artificial intelligence system, and it has been a Frontier subject of artificial intelligence in the world in recent years. In modern industry and military fields, the cooperation among agents is important. Through the cooperation among agents, the complex, difficult or high-precision tasks can be completed, In the proposed system they considered the framework in presence of both node and link attack. They initially proposed an algorithm called JLNA which is used to reduce the β-disruptor problem. But they have used the sparse cut method which has more unwanted cuts. Hence they propose an algorithm called hybrid meta-heuristic (HMM) algorithm.It is used control the difference between the connectivity in the residual graph and the target connectivity. In the proposed system we attain the reconstructed network to attain the maximum transmission without loss of the data and time consumption for the transmission. Here the process takes place with the high link cost and the less distance between the each transmission nodes.

the reliable of the system can be improved. Based on the above advantages, multivalent has been widely used in many fields, such as multirobot, multiunmanned aerial vehicle, transportation, and power system. From mathematical analysis, multivalent system is actually a complex distributed parameter system. Based on this model, we can study various collaborative control functions and complete complex tasks.The computational experiments are used to analyze and evaluate the system. Finally, the distributed parameter system is controlled and managed by parallel execution. The main contribution of this paper is to introduce the parallel control method into distributed parameter system, and the effectiveness of the proposed method is verified by the experiment. For complex distributed parameter systems, we design parallel control based on ACP method.

Experimental Result and Analysis:

The resulting errors measure the estimation error correlated to the total value of the delay. In these cases, we got an average estimation error of the CPU of 2.26% with a maximum of

4.91. The delay estimations had an average error in accuracy of 1.75% with a peak of 4.4%. This is partially due to the small size of the errors compared to the total delay as well as using monitored parameters to estimate the results of the migration.The experimental results have shown that the system has an overall accuracy of over 90% for both the Delay and Load models. Furthermore, testing on physical systems has shown that even in different scales for both the physical and virtual environment, our proposed methods provided improvements for applications meeting their constraints and reduced the overall delay of the system compared to the initial deployment scenario. The results also show that it has outperformed the Load variation based Reliability Optimization Method in terms of delay improvements, but pared on the reliability. Most importantly the Constraint based optimization method managed to clear all constraint violations for the physical system and reduced these by an average of 67% for the scaling tests.

Conclusion& Future Enhancement

In this paper, they considered the joint node and link attacks because it poses the major threat to the network. They proposed the performance to assess the vulnerability of the network. Further, have to solve the resource provision to the network and have to construct the efficient route path to attain the minimum network flow between each node. The process is experimentally evaluated in terms of real time transmission between the source and destination which are considered from the nodes those are considered as the whole network then reconstructed by the process which have satisfies the criteria in the process as the small cut ratio. In the proposed system we have improve the transmission performance by avoiding the attacked link and node. But here we need to improve the resource allowance process between the deployed in the reconstructed network. That work has to be investigating in the future work hence we can enhance the whole transmission performance based on the user priority in the deployed arrangement.

References:

[1] Key-Aggregate Cryptosystem for Scalable Data Sharing in Cloud Storage Cheng-Kang Chu, Sherman S.M. Deng, Senior Member, IIEEE TRANSACTIONS ON PARALLEL AND DISTRIBUTED SYSTEMS, VOL. 25, NO. 2, FEBRUARY 2014

[2] Collusion-Resistant Privacy-Preserving Data Mining Bin Yang_1 Hiroshi Nakagawa_2_1 Graduate School of Information Science and Technology, The University of Tokyo _2 Information Technology Center, The University of Tokyo

[3] Secure Multi-Party Computation Made Simple Ueli Maurer* Department of Computer Science ETH Zurich CH-8092 Zurich Switzerland.

[4] A Survey of Key Management for Secure Group CommunicationSANDRO RAFAELI AND DAVID HUTCHISON*Computing Department, Lancaster University.*

[5] D. Boneh and M. Franklin. Identity-based encryption from the Weil pairing. SIAM J. Com-puting, 32(3):586{615, 2003. Extended abstract in Proceedings of Crypto 2001.

[6] MertOzarar and Attila Ozgit, *Secure multiparty over-all mean computation via oblivious polynomial evalua-tion*, International Conference on Security of Informationand Networks, 2007..