Multi Node Data Transmission Analysis Based on Efficient Interruption Recognition Technique

A. Anthony Paul Raj
Research Scholar, Periyar University, Salem.
Paulraj.apr@gmail.com

J. K. Kani Mozhi
Professor,
Department of Computer Application
Sengunthar Arts and Science College,
drjkkanimozhi@gmail.com

***Abstract*- The present paper describes the network node to node network security, the present scenario reports there are numerous algorithm and technique are developed and used by the peoples for the security of network but the drawback is the time complexity is high which helps for the peoples to crack the security of various nodes and it can`t identify the peoples .This paper describes the multi node traffic analysis and load on the various nodes connectivity by sending and receiving data frequency and in specific time period by calculating weight on every node the stack time and obtain critical path it is secure transmission if not then abnormality is detected efficiently. The proposed method provides the support to sort the lacuna of existing system in less time complexity and with more accuracy**

Keywords - Interference exposure Systems, Node Analysis, weight, frequency Analysis, maximum load nodes, forward and back word frequency load analysis etc

1. INTRODUCTION

At present, network security is a great challenge for the experts due to booming of Information Technology numerous peoples became the heavy user of mobile network through land line based modem and others. The various companies are providing various space for malicious users to interrupt the network through large number of data packets towards the various nodes and succeed to drop the ratio of data packets which affects on the user network data security by making interruption the send and receiving data frequency and reduce the performance of the network.

Till now various algorithm and tools and techniques are developed to secure the network through the nodes the host based algorithms, identifies the interruption based on the details of host by maintaining a set of host which are identified as malicious. Only the host node from where the data packet is received is classified as malicious node and the node id should be present in the malicious list.

Similarly there are various rule based algorithms and tools used to identify the network interruption attack. The data packet feature has been extracted and classified and analyze by the available rule based system if any abnormality found so the specific node receiving /sending declared as malicious node but the time complexity is more.

To overcome time complexity, this paper presents multi node network analysis algorithm for efficient interruption detection. The method analyzes various features of network communication. eg: connectivity of different nodes by network path weight load, network frequency, network data packet and hosts. Based on the calculation and analysis of various features then the result is optimize and detects interruption.

The malicious user would generate huge network weight load by fake data packets to disgrace the service to the selected network node and perform interruption attack .By monitor the network weight load features of the network data packets the interruption attack can be detected with the network source node information. Similarly, the network data path analysis among nodes plays important role for interruption detection by available path, network rout and the ratio of data receiving and data sending frequency will analyze for secure network transmission among the nodes. Which will improve the accuracy of interruption detection can be performed and presented by some of the examples presented in this paper in the subsequently sections.

2. RELATED WORK

Interruption expectation acknowledgment is to translate and pass judgment on the reason, vision and aim of aggressors through dissecting an enormous number of low-level caution data, which is to give a sensible clarification of countless attack information. Recognizing attack goal can decide the genuine reason for aggressors and foresee the ensuing assault conduct, which is the reason and establishment of risk examination and the significant piece of system security circumstance mindfulness. It has become an intriguing issue in the field of system security. At the soonest, the examination of aim acknowledgment was completed in the field of man-made brainpower. Goal of operator is the picked arranging course to accomplish an objective of paper (Tahboub, 2006)Intelligent human machine interaction based on dynamic Bayesian networks probabilistic intention recognition, (X. Chai, 2005), which job is to control the

level-headed basic leadership and plan future conduct. Goal acknowledgment is the way toward apperceiving and thinking expectation of specialist. (F. Cuppens, 2002) discussed the alerts through demonstrating assault conduct. For a solitary assault conduct, the technique refined the preconditions and results of the assault. At that point the strategy associated two assault practices agreeing coordinating condition between essential of consequent conduct and results of past acts. Hence, the strategy is no compelling reason to build up assault design base, and it can find some obscure assault situation with adaptability.

Paper (P. Ning, 2003) consequently created assault technique portrayed by assault methodology chart through caution connection and the technique improved the examination of assault system by estimating the closeness between assault procedures to find the embodiment of the assault methodologies.

Paper (Z. Yanxue, Approach to forecasting multi-stage attack based on fuzzy hidden markov model, 2015) proposed a perplexing assault forecast technique dependent on fluffy concealed Markov model the techniques, investigate and correspond by abusing vulnerabilities, can thinking and foresee interruption by reproducing assaults which security examination as assault diagrams integrating the system topology, helplessness data, firewall rules and other data.

Paper (O. Sheyner, 2002) proposed application model to consequently create assault chart. Paper (S .Noel, 2005) decreased the multifaceted nature of assault diagram to effortlessly comprehend utilizing association network bunching methods.

The paper (X. Ou, 2005) actualizes strategy based multi-have, multi-step investigation of the helplessness. Model portrayal of system and rearranging the assault rules can enormously diminish an opportunity to create assault chart.

Paper (M. Alhomidi, Attack graph-based risk assessment and optimization approach, 2014) examined organize security assurance utilizing assault chart. In any case, a large portion of these techniques which are static examination can't adaptively change the age and show of assault chart dependent on genuine assaults and reaction measures. The paper (Schiffman, 2011) Disclose the Common Vulnerability Scoring System (CVSS). Paper (W. Yong, 353-362.) introduced A Network Security Situational Awareness Model Based on Information Fusion. Paper (Q. Peili, 2009) discloses Application of Honey pot in Network Security.

Paper (M. Alhomidi, Attack graph-based risk assessment and optimization approach, 2014) discloses the technique on Research and Implementation of Intrusion Detection System Merged Scanner Technique Paper (X. Chai, 2005) introduced Automatic learning of attack behavior patterns using Bayesian networks. Paper (F. Kavousi, 2012) efficient minimum-cost network hardening via exploit dependency graphs.

Paper (F. Kavousi, 2012) defines Secure Multicast Routing Protocol in MANETs Using Efficient ECGDH Algorithm. .Paper (Arepalli, 2016) shows the process on A Real-time Network Threat Recognition and Assessment Method Based on Association Analysis of Time and Space.

Paper (Lv Huiying, 2014) described Attack graph-based risk assessment and optimization approach. Paper (M. Alhomidi, 2014) shown Approach to forecasting multi-stage attack based on fuzzy hidden markov model .Paper (Z. Yanxue, 2015) made the Comparative study of SLIM+ and PUMA protocols for multicasting in Open-MANETs. Paper (Hussaini N. K., 2017) introduces M. Evolution of a Robust Multicast Routing Protocol for Open-MANETs. .Paper (Hussaini, 2017) shows the model on The Average End-to-End Delay and Average Throughput Comparison of Multicast Routing Protocols in MANETs for Real-Time Streaming.

Paper (Hussaini N. K., 2017) Evaluation of Routing Overhead of SLIM+, PUMA, and MAODV Multicast Routing Protocols in MANETs. There are many more researcher discloses various concepts on the network security. Also, the investigation of vulnerability that the likelihood of being abused of assaults brought about by various assault trouble and concealed degree isn't yet adequate.

3. MULTI NODE TRANSMISSION ANALYSIS BASED INTERRUPTION DETECTION

The presented multi node transmission analysis algorithm monitor the receiving and sending data packet traffic on the network node based on this the present process extracts the network weight features, network data receiving and sending frequency ratio , network path features and network weight node to node connectivity path load analysis and network data flow. The present method is used to envisage the true weight for the incoming data packets among nodes in terms of the numeric value to perform interruption detection.

The Figure demonstrates the architecture of future interruption detection system and it shows the various stages of interruption detection system. Each stage has been explained in detail in this section.

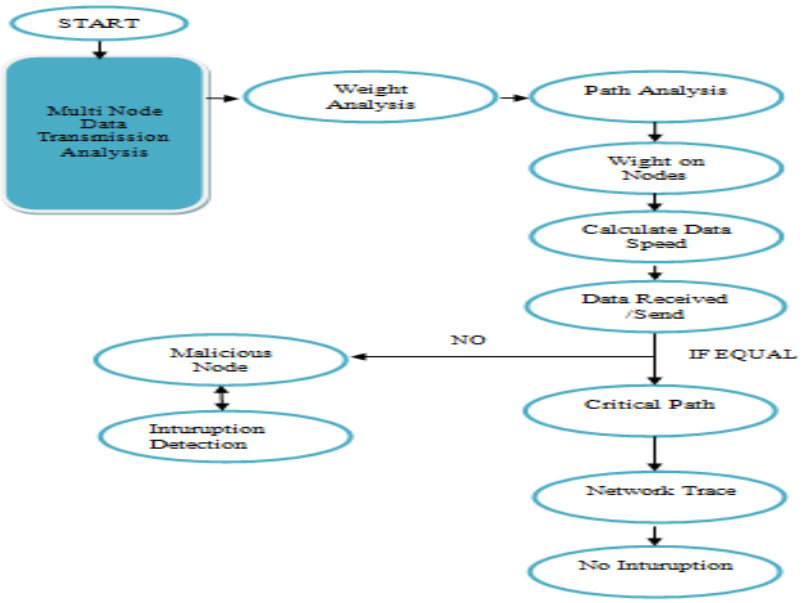

Figure 1. Architecture of Proposed Multi NODE interruption detection

3.1. *Weight load Analysis*

The network service has been accessed by different users by means of nodes in preset length. The malicious user in turn would generate packets with higher volume data. By analyzing the weight a load feature on the specific node by received data packet the check reliability of data packet the data packets are received and weight load features are extracted and the previous session of network is traced and retrieved by the different user have been from the network trace. Using the trace, the method extract the weight load features and estimates the average weight load numeric value it estimates the weight load to conclude the reliability of received data packet.

3.2. *Frequency Analysis*

The flow of data Packet's plays significant role to identify interruption attacks on the nodes of the network by the ratio of data receiving and sending frequency of data packets towards source to any node point, the interruption attack can be Compute Average weight load which shows how the weight load weight has been calculated for the receiving data packet to the node in specific time slot. The weight load feature has been calculated numerically by data received and data send and perform interruption detection at the end.

3.3. *Node Path Analysis*

The node path analysis is the process of analyzing the node path being detected. The data frequency analyze the ratio of receiving and sending data packet towards the request of required nodes and classified the users of the network. This method calculates the frequency weight towards the request to specific node as reliable user of the specific node.

4. INTERRUPTION DETECTION ALGORITHM

In this session we use some preliminary definition and mathematical formula which is used in the algorithm described as;

4.1. Network data Forward Pass (NFP)

- Network data Earliest Start Time (NES) – earliest time an Network data session can start – NES = maximum NEF of immediate predecessor
  Network data Earliest Finish time (NEF) – Network data earliest time a session can finish.
- Network data earliest start time plus activity time i.e. NEF= NES + *t*
  Network data Backward Pass (NBP) =Network data Latest Start Time (NLS) Latest time a session can start without delaying,
  Network data Latest finish time (NLF) Latest time a session can be completed without delaying Network data critical path time
- Network data critical path time NLS= NLF – *t*
- Network data Critical Path analysis:
  Analyze the paths of source nodes through the network and determine the float for each session

Three time estimates are required to compute the Network data parameters of session duration distribution:

- Network data distrustful time (NTp): the time the activity would take if data ratio having the venerability.
- Network data most liable time (NTm): the consensus best estimate of the activity's duration
- Network data hopeful time (NTo): the time the activity would take if no venerability occurred then
- Mean (predictable time): NT*e* = (Ntp + 4 NTm +NTo)/6

4.2. Algorithm:

The proposed interruption detection algorithm reads the receiving data packet and extracts features like network weight load, network path and data frequency values in numeric form and analysis returns a weight measure and computes the multi node trust weight for the receiving/sending data packet classifies the data packet as genuine or malicious to perform intrusion detection on the node.

4.3. Main Algorithm:

Step 1: Start
Step2: Fix Network beginning time and system load on the hub =0
Step3: Compute numerically number of accepting information parcel (data ratio) on the hub
Step4: Compute numerically number of information sending proportion
Step5: Calculate path load
Step6: Compute numerically hub weight forward as far as information parcel accepting by most extreme load= load
on the hub + path load
Step7: Repeat the stage 6 till end hub is spread
Step8: Compute the retrogressive burden as far as information sending proportion by load on the hub and weight on
the way for example (Back word load = min(weight on the gesture – weight on the way))
Step9: Repeat step till the beginning hub is secured for example on the beginning hub forward load=back word load
are zero so distinguish net work is right
Step10: Notify the hubs where the advance and back word load are rise to so distinguish that no interference for
example basic way so sheltered hubs
Step11: If load are not rise to by methods for various loads on the gestures so distinguished interference on the hubs
Step12: Stop

5. RESULT AND DISCUSSION

Example: The network data described in table 1 and try to find out the network - critical path with the help of above algorithm for convince the 27 nodes data is collected at specific time.

Step 1: Compute network time parameters of each node and session
Step 2: Compute network total float of each session and network total floats of network non-critical activity to the node (N3, N7) is positive maximal ones.
Step 3: Find out the network least duration path
Step 4: Find out the least duration network path N1→ N 3
Step 5: Find out the network least duration path is that N7→N12→N17→N22→N27
Therefore the network shrink critical path
N1→N3→N7→N12→N17→N22→N27
And its network length is =520-174 =346 clearly shown by the table Data is collected randomly from the network trace for 27 convenient nodes represent N1,N2,N3,N4,N5,N6……N27 and arranged in tabular column as follows

Table 1. Network Data

Network Node	Network Path load	Receiving Data packet	Sending data packet
N1-N2	140	140	164
N1-N3	80	80	101
N1-N4	120	120	120
N1-N5	110	110	140
N1-N6	100	100	120
N2-N7	100	240	264
N2-N8	40	180	220
N3-N8	30	180	220
N3-N9	110	210	210
N4-N9	90	210	210
N4-N8	30	180	220
N4-N10	80	200	200
N5-N10	60	200	200
N5-N11	90	200	240
N6-N10	80	200	200
N6-N11	70	200	240
N7-N12	60	300	324
N7-N13	10	250	250
N8-N13	30	250	250
N8-N14	50	270	270
N9-N14	59	270	270
N9-N15	30	240	260
N10-N15	10	240	260
N10-N16	50	250	300
N11-N15	20	240	260
N11-N16	40	250	300
N12-N17	110	410	434
N12-N18	10	310	370
N13-N17	100	410	434
N13-N18	60	310	370
N13-N19	10	300	300
N14—N19	30	300	300
N14-N20	50	320	332
N15-N19	10	300	300
N15-N20	60	300	300
N15-N21	100	340	360

N16-N20	30	320	332
N16-N21	60	340	360
N17-N22	70	480	504
N17-N23	10	420	480
N18-N22	100	480	504
N18-N23	80	420	480
N18-N24	30	400	400
N19-N24	20	400	400
N19-N25	110	410	412
N20-N24	60	400	400
N20-N25	80	410	412
N20-N26	20	390	410
N21-N25	50	410	412
N21-N26	50	390	410
N22-N27	16	520	520
N23-N27	40	520	520
N24-N27	120	520	520
N25-N27	108	520	520
N26-N27	110	520	520

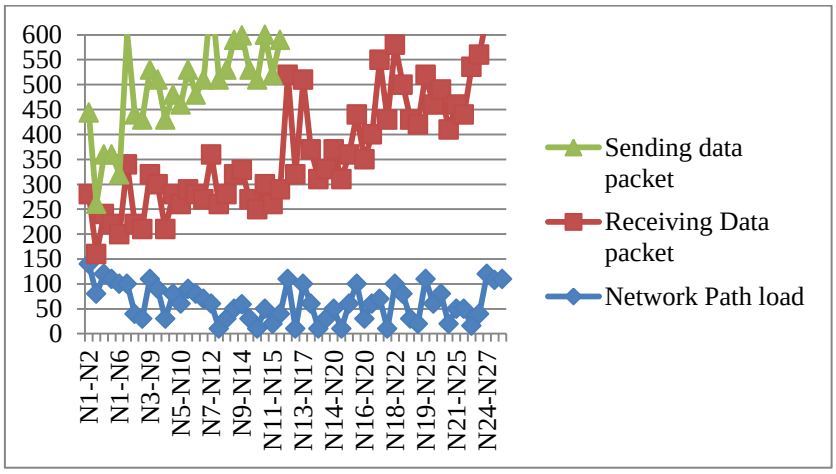

Figure 2. Graph for finding network critical path for 27 nodes

The graph X-axis shows Nodes, Y axis shows - Network Path load, Receiving Data packet, Sending data packet. So from the figure 2, it is clear that the network critical path is among the nodes N1-N4-N9-N14-N19-N24-N27 because these having the ratio of data sending and receiving are equal data so by algorithm it is clear theses nodes are safe else the other nodes having the variation in data ratio so it can be treated as malicious nodes.

6. CONCLUSION

The problem of interruption detection in network systems has been approached with the multi node transmission analysis algorithm presented in this paper. The method monitors the incoming traffic and extracts the network weight load, network path and receiving and sending data frequency features. Each feature has been analyzed for their reliable by measuring the network frequency weight for the feature considered. Based on the numeric values returned at each analysis, the method estimates the multi node trust weight based on which the method performs interruption detection. The proposed algorithm has improved the performance of interruption detection accuracy at different conditions considered. The false detection ratio has been minimized with improved time complexity.

REFERENCES

Arepalli, G. E. (2016). Secure Multicast Routing Protocol in MANETs Using Efficient ECGDH Algorithm. *International Journal of Electrical and Computer Engineering (IJECE), 6*(4), 1857–1865.

F. Cuppens, F. A. (2002). Recognizing malicious intention in an intrusion detection process. *Proceedings of the 2nd International Conference on Hybrid Intelligent Systems.*

Hussaini, N. K. (2017). Evolution of a Robust Multicast Routing Protocol for Open-MANETs. *Sindh University Research Journal-SURJ (Science Series), 49*(1), 219-224.

Hussaini, N. K. (2017). The Average End-to-End Delay and Average Throughput Comparison of Multicast Routing Protocols in MANETs for Real-Time Streaming. *Sindh University Research Journal-SURJ (Science Series), 49*(2), 329-334.

Hussaini, N. N. (2016). A Comparative study of SLIM+ and PUMA protocols for multicasting in Open-MANETs. *International Journal of Computer Science and Network Security (IJCSNS), 16*(12), 128-131.

Lv Huiying, P. W. (2014). A Real-time Network Threat Recognition and Assessment Method Based on Association Analysis of Time and Space. *Journal of Computer Research and Development*, 1039-1049.

M. Alhomidi, M. R. (2014). Attack graph-based risk assessment and optimization approach. *International Journal of Network Security & Applications, 6*, 31-43.

M. Alhomidi, M. R. (2014). Attack graph-based risk assessment and optimization approach. *International Journal of Network Security & Applications, 6*, 31-43.

O. Sheyner, J. H. (2002). Automated Generation and Analysis of Attack Graphs. *Proceedings of the 2002 IEEE Symp on Securtiy and Privacy.*

P. Ning, D. X. (2003). Learning attack strategies from intrusion alerts. *Proceedings of the 10th ACM Conference on Computer and Communications Security.*

Q. Peili, S. P. (2009). Research and Implementation of Intrusion Detection System Merged Scanner Technique. *Journal of Harbin University of Science and Technology*, 5-59.

Q. Peili, Y. Y. (2009). Study on Application of Honeypot in Network Security. *Journal of Harbin University of Science and Technology*, 37-41.

S .Noel, S. J. (2005). Understanding complex network attack graphs through clustered adjacency matrices. *Proceedings of the 21st Annual Computer Security Applications Conference.*

S. Noel, J. O. (2003). Efficient minimum-cost network hardening via exploit dependency graphs. *Proc of the 19th Annual Computer Security Applications Conference, CA: IEEE Computer Society.*

Schiffman, M. (2011). Common Vulnerability Scoring System (CVSS). Retrieved from http://www.first.org/cvss/cvss-guide. html

Tahboub, K. A. (2006). Intelligent human-machine interaction based on dynamic Bayesian networks probabilistic intention recognition. *Journal of Intelligent and Robotic Systems*, 31-52.

Tahboub, K. A. (2006). Intelligent human-machine interaction based on dynamic Bayesian networks probabilistic intention recognition. *Journal of Intelligent and Robotic Systems*, 31-52.

W. Yong, L. Y. (353-362.). A Network Security Situational Awareness Model Based on Information Fusion. *Journal of Computer Research and Development.*, 2009.

X. Chai, Q. Y. (2005). Multiple-goal recognition form low-level signals. *Proceedings of the 20th National Conference on Artificial Intelligence*, (pp. 9-13.).

X. Ou, S. G. (2005). MulVAL: A logic-based network security analyzer. *Proceedings of the 14th Usenix security Symp.*

Z. Yanxue, Z. D. (2015). Approach to forecasting multi-stage attack based on fuzzy hidden markov model. *Electronics Optics & Control*, (pp. 39-44).

Z. Yanxue, Z. D. (2015). Approach to forecasting multi-stage attack based on fuzzy hidden markov model. *Electronics Optics & Control, 22*, 39-44.