ISSN:0975-9646

A Literature Review on Security Aspects for Fault Tolerance in Networks

[1] Kavita Mishra [2.] Prashant Vats

[1,2]*HMRITM,*
New Delhi, India

Abstract: The security aspects and fault tolerance of the computational network provides have a crucial impact on the designing and use of networks. It provides the framework for securing the networks with the unwanted faults and to increases the reliability of the fault tolerance network. The conceptual view for provide secure the networks and diagnose the faults. In this paper we have carried out a literature review of the application of security and fault tolerance into various areas of computational network problems. We have further carried out a tabular comparison of the work performed by the various researchers for applying the various aspects of security into the fault tolerance networks.

Keywords: Fault tolerance, security, WSN, voters.

I. INTRODUCTION

Fault tolerance & security is an area which emphasis on how we secure networks and continuous work with the presence of the faults into any existing computational networks .Network security increases the throughput of the network and helps to reduce the faults. Fault tolerance is used to resolve the faults, errors and failure and increase the speed of the system when an error is introduced.

Security and fault tolerance is designed for enhancing the reliability with the higher data transmission rates.

Higher availability & higher reliability are the main features of the fault tolerance which allows the system to work with faults and errors. These approaches examine the network security based on the fault tolerance for the high security of the networks. It uses encryption & decryption methods for securing data & packet transmission and thus reduces the risk of failures. It increases the security of all the network systems to avoid unauthorized access and use.

In this paper we have reviewed the work carried out by various researchers on the security aspects of fault tolerance in networks and their applications into various domains. In the second section of the paper we have presented a literature review of various applications of security and fault tolerance towards providing of their real time scenarios. In the third section we have made a comparative analysis for the application of fault tolerance and security based on certain parameters with their comparison presented in a tabular format. In the fourth section we have carried out our conclusion about the solutions of the networks problem. In the fifth section of the paper, we have discussed the future work related to security aspects of the networks.

II. LITERATURE REVIEW

Author Zvi G.et.al.,[1] has proposed there was to designing protocols to solve the multi -party computation problems for the various subjects & various cryptographic constants for the faulty networks. The fault tolerance of this method is used when a fault is detected during the execution time, faulty protocol can lose its identity completely and at the same time another user secures, shares and reconstructs it's input & output domain. Its involves the security and reliability in which at the time when fault is detected the protocols are not changed but distribution can be used to preserve the security & privacy of all the user or multi-parties without losing the information of protocols. The advantage of this method is correctness, synchronization, privacy and trusted party mythology. Disadvantage of this method is if the first and second party cannot generate their trapdoor functions then the third party cannot use the function of encryption for the computational results. It is implementing in minimum knowledge protocol.

Li Shu [2] has proposed high reliability of data storage by lowering the degree of redundancy in system & subsystems. In fault tolerance a protocol layer inserted between two layers of a communication system can monitor & analyze the network links and to provide a secure data transmission. It use Mobile ad hoc network (MANET) along with encryption key which enhances security and reliability depends upon the multiple message segments sent in the network. It achieves high reliability; we can use redundant array of independent disk (RAID) subsystem which protects the system in case of any failure. Disadvantage of this is cost ineffectiveness, insufficient and data duplicacy in more than one system. Future research is needed to consider encryption and scrambling technique can be used to improve security.

Erland Jonson [3] shows the relationship between behavioral viewpoint and preventive system as well as traditional security with the exciting dependability concepts. In this if one system fails the information get transferred to other system with proper safety and security. For the security & reliability use of formal models and system protection rule for integrity based access control matrix. The advantage of integrity is used to prevent the unauthorized modification and also protects the system from any abnormal attacks. Confidentiality is the main

demerits of this method because using this non user can access the system to an extent though limited. Confidentiality needs to be improved in future for high integrity and fault preventions.

Mark K.Joseph, et al.,[4] has proposed how virus can spread throughout a network or a computer system using the authorization of the user. Faults are handled by the fault classes and when they occur, the run time mechanism is designed to tolerate them. For the security, fault tolerance techniques are used to retrieve the address of random faults and rollback procedure identifies it. NVP (N-Version programming) provides reliable software of fault tolerance. PFM uses backward recovery mechanism to detect the control flow error but PFM schemes cannot be used to detect the deliberate faults. It is implemented in Trojan Horse tool. For the future, we can purpose a secure computing system having cost effective design.

Sahel Alouneh, et al.,[5] has proposed and focused on path protection fault tolerance schemes as well as issues in MPLS (Multi-protocol label switching) network and steps to resolve it. MPLS networks are prone to failures thus fault tolerance is important as it focuses on factors like utilization, recovery time and packet loss. MLPS provide VPN functionality to increase security. The advantages of this method are high speed packet delivery, reduction in PSL (Path switching LSR), fast and cost effective notification. But packet loss factor depends upon the various approaches without any guarantee from VPN and it is the disadvantage of this method. Further works needs to be data integrity, confidentiality, authentication in MPLS and multi path routing.

Moushumi Sharmin,et al., [6] has proposed to design a resource discovery unit used to maintain privacy, resource sharing and modification scheme in an effective computing environment. Fault tolerance techniques uses secret sharing in which the process will not keep a single copy of resource manager to ensure the optimum use of tiny storage. For the security & reliability resource provider provides privacy and security to a specified resource and resource holder is responsible for providing it to approved person only. Resource manager manages resources, facilitates the best match and stores the address in the hash table. Disadvantages are in this increases seek time, wastage of resources & memory, low privacy of service information and domain identity. It is implemented in Cellular Automata. To resolve the QoS issues, increase the seek time and focus on resource information for the future purpose.

M.AI-Kuwaiti et.al., [7] has proposed address issues of complex infrastructure such as information, reliability and availability with some fault tolerance and security features. In fault tolerance the system behaves normally in case of any hardware or software fault and fault masking is another method that can be used to tolerate fault. Reliability refers to any failure free operation during an interval and security protects confidentiality & integrity. Its advantage is that good approach for network design and packet transfer and optimize the design using major factors. Dependability, duplicacy and higher failure rate are the demerits of this approach. Future purpose is to increase security & availability features.

Ben Hardekopf,et al., [8] has proposed a system with security and fault tolerance in case of congestion and protocols to create a secure voting algorithm. Durability & Redundancy is used to reduce the risk of any single component in operating flawlessly is the advantage of this approach. Future work is that reduce network congestion, reliability & security for the WAN.

Jitendra K. Rout, et.al.,[9] has proposed a fault tolerance paradigm that can identify the black holes attack which degrades the performance of the network by dropping the packets. In the fault tolerance dividing the routing protocols into zones, if an error occurs in one then the other zones does not get effected and a node connection algorithm is used to detect where the fault has actually occurred. For the security purpose network connection algorithm used for fault tolerance and provide reliability. Its advantages are that many routing protocols have been discovered because of which data transmission and maintenance has been enhanced. Due to this increase in the number of routers, bandwidth and cost will be effective. It is implemented in Route discovery and node connection algorithm. The future purpose is to implement SFT algorithm, reduce packet delivery time and increase the throughput.

Steven E.Crerwinski et.al., [10] has proposed to handle the failure automatically by hiding the complexity of fault recovery and to determine whether the communication among the components is secure or not. For the fault tolerance whenever a packet gets dropped, cryptographic methods provide strong authentication at end points. SDS server is used to calculate the number of clients in the system and verify that the security features of the system does not reduced and Authenticated RMI implementation is used to encrypt the data sent over the network. Its advantages are that it scalable, secure information repository and fault tolerant. Lack of access control, service information cannot be granted and cost in effective. It is implemented with JINI and XML. Focusing on directory services, security features of the system and explosive growth of networks are the future perspectives.

Yaron Minsky et al., [11] has proposed a variety of applications in the internet and other large distributed systems. Replication and voting are not sufficient for improving the performance of agent computation. It involves fault tolerance, if there exists no faulty host in the pipeline then the remaining hosts separate the computations by sending an agent. The correctness of the present state depends upon the correctness of predecessor. It uses chain of authentication to prevent masquerading and when two hosts combine then voting will determine which faulty host is encountered and which is not, it is used for security factor . Advantage of this approach is that VSS scheme allows for the correct reconstruction of assets and cryptography demerits for this approach is insufficient

protocol, voting performance, high cost and synchronization delay. Improve voting and cost performance.

Stephen Bohacek et.al.,[12] has proposed simulation that improves routing security, minimize the impact of link router and approaches to failure prevention and recovery. Used dynamic routing protocol to try to reduce the failure, when a fault is generated in one layer then transmission will keep following the same route and continue interception. Security contains protest against some form of interception; provide end to end security mechanism to other layers. Its advantages are to improve security and fault tolerance; proactive approaches to achieve connectionless value enable failure. Demerits are increasing throughput and complex multiple parts. For future work, scalable algorithm is required to compute next hop probabilities, decrease packet transmission delay and increase throughput.

Bharat B. Madan,et.al., [13] has proposed assessment of security attributes for an intrusion tolerates system. Fault tolerance ensures the effective recovery from failures and allows a finite probability; the system security may be breached. SMP model deals with security, Integrity and authorized actions. Merits are it is able to detect faults in the system and detect the insertion of the security attacks into a system. Various subsystems communicate with each other. But it can't compromise with data integrity and DOS attacks, consume large amount of service resources. It is implemented in SITAR. In the future, it can consider quality and security attributes, cost and can determine the inside system strength and weakness.

Kevin J.Rowett [14] has proposed to various fault tolerance designs such as redundancy part, data checking and multi-port transmission. In the fault tolerance the pair of network control device sends a message to the provider of the other pair of the network and identifies the other pair of network which operates continuously. It is for secure & reliable hub to hub connection to transmit data and provide fault redundant network. Its advantage is that high availability computing system, stores and maintains the resources. Increases number of ports. Extents the work in fault tolerance technique, provide multi- processor and increase availability.

David Tipper et.al.,[15] has proposed survivability framework and focuses on voice service network. It generates wireless access network and reliability. When fault occurs user provides continuous service and non-user cannot access the system without authentication. Mitigate the impact of failures. Cost issue, long distance, range problem and no network are the main problems in this approach. It implements in Checkpoint algorithm. It is for the future perspective to extend the scope of services.

Daniel F. Macedo, et.al., [16] has proposed misfortune of routing protocol for continues data to deflect WSN and shows performance of routing protocol. In fault tolerance EAD, PRO and TinyoS are used to reduce faults & failure can be calculated using the probability of packet lose. No security protocol can be evaluated and techniques are used for denial of service attacks for the reliability. Its advantage is PROC which determines the failed route and EAD are used to maximize the number of leaf nodes. Processor crashes, energy depletion and failures due to security attacks are the disadvantages of this approach. Future study done in QoS parameter affected by failures and verification of these in faulty scenario.

Fred B. Schneider [17] has proposed characterizing security policy, enforcing them and implementing its connections with fault tolerance agents. For fault tolerance, masking the effects which executes an agent of faulty processor replication and voting is considered. After reading the files no message will be sent. By improving security and reliability we use secure automata properties. Its advantage is that detect bogus agents and sender authentication. Demerits approaches protocols Inefficient and constant size message. It is implemented in Automata. Future needs to enforce security policy system.

A.S Alvi et.al.,[18] has proposed to improve the framework servers, security techniques and provide functional & secure system. Fault state table is used for checking the fault conditions in each sever application and switching the application server to the self -healing manager. Self -tuning & self- healing methods are used to recover the data which is affected by the operational faults and it is useful for security as well as reliability. Authentication, reliability, availability & integrity are the main merits of this approach. Server survivability are the demerits of this approach. Future work needs to enhance the consistency& survivability of the server and improves the cloud data storage. RSA algorithm is used for implementation.

Yi Gu,Qishi Wu [19] has proposed to optimize the large scale data transmission and manage the distributed workflow with high throughput require runtime recovery in case of resource failure during the workflow execution. Mapping is used security & reliability for assigning each module for the workflow. This approach is used for achieving maximum throughput and minimizes the failure. Not suitable for long execution and increased the size of computer networks is the demerit of this approach. Invent backup mechanism for recovery and identify the mapping problem with multi workflow.

James D.Allen[20] has been proposed to improve performance for multi-computer, link tolerance and router failures. PCS used for reduce fault occurrence and used for high data transmission rates. Using this approach, enhance the performance of the routers. Its demerits are that it does not support virtual channel transmission.

III. A TABULAR COMPARISION OF SECURITY ASPECTS FOR FAULT TOLERANCE IN NETWORKS

In this section of the paper, we carried out a tabular analysis of security for fault tolerance in networks application into various aspects of network domain and have presented it in Table 1.

TABLE 1. A TABULAR COMPARISION OF SECURITY ASPECTS FOR FAULT TOLERANCE IN NETWORKS

S.N	Author	Issue address	Fault Tolerance	Type of Networks	Security & Reliability	Merits	Demerits	Tools/Algo.	Future Work
1.	Zvi Gali, Stuart Haber(1988)	Proposed to design protocols to solve the multi-party computation problems & subjects to various cryptographic constants	When a fault is detected during the execution time faulty protocol can lose its identity completely and at the same time another user secures shares and reconstructs it's Input & output domain.	Cryptographic computation	At the time when fault is detected the protocols are not changed but distribution can be used to preserve the security &privacy of all the user or multi parties without losing the information of protocols	Synchronization. Correctness, privacy and trusted party mythology	If the 1st and 2nd party cannot generate their trapdoor function together then the 3rd party cannot use the function of encryption for the computational results.	Minimum knowledge protocol	------
2.	Li Shu (2003)	To propose high reliability of data storage lowering the degree of redundancy in systems & subsystems	A protocol layer inserted b/w two layers of a communication system can monitor & analysis the network links and provides a secure data transmission.	Distributed networks	Using MANET along with encryption key enhances security and reliability depends upon the multiple message segments sent in the network.	To achieve high reliability we can use RAID subsystem which protects the systems in case of any failure.	Cost ineffective, inefficient & data duplicacy in more than one system.	--------	Encryption and scrambling technique can be used to improve security.
3.	Erland Jonson (1999)	It shows the relationship b/w behavioral viewpoint and preventive system as well as traditional security with the exciting dependability concepts	If one system fails the information get transferred to other system with proper safety and security.		Use of formal models and system protection rule for integrity based access control matrix.	Integrity is used to prevent the unauthorized modification and also protects the system form any abnormal attacks.	The Non users can access the system to an extent though limited, this is known as confidentiality	---------	Confidentiality needs to be improved further for high integrity and fault prevention.
4.	Mark K.Joseph,Algirdas Avizienis (1988)	To proposed how virus can spread throughout a network or a computer system using the authorization of the user.	Faults are handled by the fault classes and when they occur, the run time mechanism is designed to tolerate them.	Computer viruses	Fault tolerance techniques is used to retrieve the address of random faults and rollback procedure identifies it.NVP provides reliable software of fault tolerance.	PFM uses backward recovery mechanism to detect the control flow error.	PFM schemes cannot be used to detect the deliberate faults.	Trojan Horse tool to be used.	Creating a secure computing system having cost effective design.
5.	Sahel Aloune	Focused on path protection fault tolerance schemes as well as the issues in MPLS network and steps to resolve it.	MPLS networks are prone to failures thus fault tolerance is important and it focuses on factors like resource utilization, recovery time and packet loss.	MPLS	MPLS provides VPN functionality to increase security.	High speed packet delivery, reduction in PSL, fast and cost effective notification	Packet loss factor depends upon the various approaches without any guarantee from VPN.	-------	Data integrity, confidentiality, authentication in MPLS networks and multipath routing.

S.N	Author	Issue address	Fault Tolerance	Type of Networks	Security & Reliability	Merits	Demerits	Tools/Algo.	Future Work
6.	Moushumi Sharmin ,Shameed Ahmed	Proposed to design a resource discovery unit used to maintain privacy, resource sharing and modification scheme in an effective computing environment.	Used secret sharing in which the process will not keep a single copy of resource manager to ensure the optimum use of tiny storage.		Resource provider provides privacy and security to a specific resource and resource holder is responsible for providing it to approved persons only.	Resource manager manages resources, facilitates the best match and stores the address in the hash table.	Increases seek time, wastage of resources and memory, low privacy of service information and domain identity.	Cellular Automata	To resolve the QoS issues ,increase the seek time and focus on resource Information.
7.	M. AI-Kuwaiti, N.Kyriakopolos and S. Hussain(2009)	Propose address issues of complex infrastructure such as information, reliability and availability with some fault tolerance and security features.	The system behaves normally in case of any hardware or software fault and fault masking is another method that can be used to tolerate fault.		Reliability refers to any failure free operation during an interval and security preserves confidentiality, integrity and attributes such as authenticity and non-repudiation.	Good approach for network design and packet transfer, optimize the design using significant factors.	Dependability, duplicacy, failure rate	---	Increase security features and availability features
8.	Ben Hardekopf, Kevin Kwait(2001)	To propose a system with security and fault tolerance in case of congestion and also propose protocols to create a secure voting system.	Multiple voters can work independently , compute their results and work to majority	Distributed systems	Authentication technique are used to enforce the secure communication without increasing the complexity of the buffer.	Durability and redundancy is used to reduce the risk of any single component in operating flawlessly.	Consume more bandwidth than distributed voting, network congestion	----	Reduce network congestion ,reliability and security for the wide area networks
9.	Jitendra Kumar Rout, Saurav Kumar Bho(2013)	To propose a fault tolerance paradigm that can identify the black holes attack which degrades the performance of the network by dropping the packets?	Dividing the routing protocols into zones, if an error occurs in one then the other zones does not get effected and a node connection algorithm is used to detect where the fault has actually occurred.	MANET	Network connection algorithm used for fault tolerance and provide reliability.	Many routing protocols have been discovered because of which data transmission and maintenance has been enhanced.	Increase in the number of routers, bandwidth and it is cost ineffective.	Route discovery and node connection algorithm.	To implement SFT algorithm, reduce packet delivery time and increase the throughput.
10.	Steven E. Czerwinski, Ben Y. Zhao, Todd D. Hodes, (1999)	Propose to handle the failure automatically by hiding the complexity of fault recovery and to determine whether the communication among the components is secure or not.	Whenever a packet gets dropped, cryptographic methods provide strong authentication at end points.		SDS server is used to calculate the number of clients in the system and verify that the security features of the systems does not get reduced and Authenticated RMI implementation is used encrypt the data sent over the network.	Scalable, secure information repository and fault tolerant.	Lack of access control, service information cannot be granted and cost in effective.	JINI and XML	Focusing on directory services, security features of the system and explosive growth of networks.

S.N	Author	Issue address	Fault Tolerance	Type of Networks	Security & Reliability	Merits	Demerits	Tools/Algo.	Future Work
11.	Yaron Minsky, Robbat Van (1996)	Propose a variety of application in the internet and other large distributed systems. Replication and voting are not sufficient for improving the performance of agent computation.	If there exists no faulty host in the pipeline then the remaining hosts separate the computations by sending an agent. The correctness of the present state depends upon the correctness of predecessor.	Distributed computing	Use chain of authentication to prevent masquerading and when two hosts combine then voting will determine which faulty host is encountered and which is not.	VSS scheme allows for the correct reconstruction of assets and cryptography.	Insufficient protocol, voting performance, high cost and synchronization delay.	--------	Improve voting and cost performance.
12.	Stephen Bohacek, Junsolee	Simulation that improves routing security, minimize the impact of link router and approaches to failure prevention and recovery.	Used dynamic routing protocol to try to reduce the failure, when a fault is generated i.n one layer then transmission will keep following the same route and continue interception	Computer networks	Protest against some form of interception; provide end to end security mechanism to other layers.	Improves security and fault tolerance, proactive approaches to achieve connectionless value enable failure.	Increase throughput and complex multiple parts.	-----	Scalable algorithm to compute next hop probabilities, decrease packet transmission delay and increase throughput.
13.	Bharat B. Madan, Katrina Goseva(2004)	Assessment of security attributes for an intrusion tolerates system.	Fault tolerance ensures the effective recovery from failures and allows a finite probability, the system security may be breached.	Distributed network	SMP model deals with security, Integrity and authorized actions.	Able to detect the faults in the system and detect the insertion of the security attacks into a system. Various subsystems communicate with each other.	Compromise of data integrity and DOS attacks, consume large amount of service resources.	SITAR	To consider quality and security attributes and determine inside system strength and weakness, cost analysis.
14.	Kevin J.Rowett (1995)	Proposed to various fault tolerance designs such as redundancy part, data checking and multi-port transmission.	The pair of network control device sends a message to the provider of the other pair of the network and identifies the other pair of network which operates continuously.	Local area Networks	Hub to hub connection to transmit data and provide fault redundant network.	High availability computing system, stores and maintains the resources.	Increase number of ports.	----------	Extents the fault tolerance technique, provide multi-processor and increase availability.
15.	David Tipper, Teresa Dahlberg and Hyundoo shin (2002)	Survivability framework and focus on voice service network.	It generates wireless access network and reliability.	Wireless access network	When fault occurs user provides continuous service and non user cannot access the system without authentication.	Mitigate the impact of failures.	Cost issue, long distance , range problem and no network connection	Checkpoint algorithm	To extend the scope of services

S.N	Author	Issue address	Fault Tolerance	Type of Networks	Security & Reliability	Merits	Demerits	Tools/Algo.	Future Work
16.	Daniel F. Macedo, Luiz H.A. Correia and Aldri L.dos Santos (2005)	Misfortune of routing protocol for continues data to deflect WSN and shows performance of routing protocol.	EAD, PRO and TinyoS are used to reduced faults & failure and failure can be calculated using the probability of packet lose.	Wireless sensor	No security protocol can be evaluated and techniques are used for denial of service attacks.	PROC used to determine the failed route and EAD is used to maximize the number of leaf nodes.	Processor crashes, energy depletion and failures due to security attacks.	---------	Study on QoS parameter effected by failures and verification of these in faulty scenario
17.	Fred B. Schneider (1997)	Charactering security policy, enforcing them and implementing its connections with fault tolerance agents	For masking the effects of execute an agent of faulty processor replication and voting are considered	Distributed systems	After reading the files no message will be sent. Improve security and reliability we use secure automata properties.	Detect bogus agents and sender authentication	Protocols Inefficient and constant size message	Automata	Enforcing security policy system.
18.	A.S Alvi, Omparkash A. Jaisinghani (2014)	Proposed to improve the framework servers, security techniques and provide functional & secure system.	Fault state table is used for check the fault conditions in each sever application and switch the application server to the self -healing manager.	Self-tuning servers	Self -tuning & self-healing methods are used to recover the data which is affected by the operational faults.	Authentication, reliability, availability & integrity.	Server survivability	RSA algo.	Enhance the consistency& survivability of the server and improves the cloud data storage.
19.	Yi Gu,Qishi Wu (2013)	Proposed to optimize the large scale data transmission and manage the distributed workflow with high throughput.	Runtime recovery in case of resource failure during the workflow execution.	Distributed networks	Mapping is used security & reliability for assigning the each module for the workflow.	Achieve maximum throughput and minimize the failure.	Not suitable for long execution time and increase the size of computer networks.	------	Invent backup mechanism for recovery and identify the mapping problem with multi workflow.
20	James D. Allen,Patrick T. Gaughan (1994)	Improve performance for multi-computers, link tolerance and router failures	PCS used for data transmission and reduce congestion during execution time.	Multi computers network	Backtracking & pipeline communication use for reliable data transfer and consume less tie for data transfer.	Performance evaluation, asynchronous router.	Not support virtual channel transmission.	--------	Improve virtual channel performance & increase protocol reliable communication.

IV. CONCLUSION

In this paper, we have carried out a survey on the various Security Aspects for the Fault Tolerance in Networks and its application into various domains. Further, we have also carried out a comparative analysis our survey. After review of we can conclude that Security Aspects are proven to be useful in providing effective solutions for resolving the issues related to the faults in a given network.

V. FUTURE WORK

Based on the above discussion, as future work we can direct our research towards Quality of Service issues, cost effective and confidentiality needs to be improved. Encryption techniques used to make a highly secure system and also workout to reduce the seek time.

REFERENCES

[1] Zvi Galil, Stuart Haber "Cryptographic computation: Secure Fault-Tolerance Protocols and the Public-Key Model" published C. Pomerance (Ed.): Advances in Cryptology - CRYPT0 *'87,* LNCS 293, pp. 135-155, 1988.

[2] Li Shu "Distributed fault tolerance & secure storage", published by US2003/0084020 A1(43) Pub. Date: May 1, 2003.

[3] Erland Johnsson "An Integrated Framework for Security and Dependability" published 1998 NSPW 9/98, Chariottsivlle,VA,USA.

[4] Mmk K. Joseph and Algirdas AviiZienis "A fault tolerance approach to computer viruses" pub. In CH2558-5/88/0000/0052$01 .00 01988 IEEE.

[5] Sahel Alouneh, Sa'ed Abed "Fault Tolerance and Security Issues in MPLS Networks" pub. ISSN: 1792-4863 ISBN: 978-960-474-231-8.

[6] Moushumi Sharmin, Shameem Ahmed, and Sheikh I. Ahamed " SAFE-RD (Secure, Adaptive, Fault Tolerant, and Efficient Resource Discovery) in Pervasive Computing Environments".

[7] M. Al-Kuwaiti, N. Kyriakopoulos "A Comparative Analysis of Network Dependability,Fault-tolerance, Reliability, Security, and Survivability" pub.in IEEE communication surveys & tutorials, VOL. 11, NO. 2, SECOND QUARTER 2009.

[8] Ban Hardekopf,Kevin Kwiat"Secure and Fault –Tolerant Voting in Distributed Systems" published by 0-7803-6599-2/01/$10.00 _ c 2001 IEEE.

[9] Jitendra Kumar Rout, Sourav Kumar Bhoi "SFTP: A Secure and Fault-Tolerant Paradigm against Blackhole Attack in MANET" pub.in International Journal of Computer Applications (0975 – 8887) Volume 64– No.4, February 2013.

[10] Steven E. Czerwinski, Ben Y. Zhao "An Architecture for a Secure Service Discovery Service" pub. In Mobicom '99 Seattle Washington USA Copyright ACM 1999 I-58113-142-9/99/08.

[11] Yaron Minsky, Robbat Van Revesse "cryptographic support for fault tolerant distributing computing".

[12] Stephan Bohacek, Jo.ao Hespanha" Game Theoretic Stochastic Routing for Fault Tolerance and Security in Computer Networks".

[13] Bharat B. Madan, Katerina Goševa-Popstojanova "A method for modeling and quantifying the security attributes of intrusion tolerant systems" pub.in 0166-5316/$ – see front matter © 2003 Published by Elsevier B.V.

[14] Kelvin J.Rowett "Method and apparatus for fault tolerance connection of a computing system to local area network", published by US005448723A Pub.Date: Sep. 5, 1995.

[15] David Tipper, Teresa Dahlberg "Providing Fault Tolerance in Wireless Access Networks" pub.in IEEE Communications Magazine • January 2002.

[16] Daniel F. Macedo, Luiz H. A. Correia "Evaluating Fault Tolerance Aspects in Routing Protocols forWireless Sensor Networks" pub. In Fourth Annual Mediterranean Ad Hoc Networking Workshop, 2005.

[17] Fred B. Schneider "Towards Fault-tolerant and Secure Agentry" pub. In 11th International Workshop on Distributed Algorithms, Saarbriicken, Germany, Sept.1997.

[18] A. S. Alvi and Omprakash A. JaisinghaniḂ "Fault-Tolerance and Transformation Analysis in Self-Tuning Servers"pub.in International Journal of Current Engineering and Technology, Vol.4, No.3 (June 2014).

[19] Yi Gu · Chase Qishi Wu "Distributed Throughput Optimization for Large-Scale Scientific Workflows Under Fault-Tolerance Constraint" pub. In © Springer Science+Business Media Dordrecht 8 June 2013.

[20] James D.Allen, Patrick T.Gaughan "Ariadne-an adaptive router for fault tolerant multicomputer". In Pro. of the Iinternational Symposium on Computer Architecture (ISCA), pages 278-288, Chicago 1994.