International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-9 Issue-3, February 2020

Improved Caching and Trust based Reliable Mobile Communication in Distributed Environment

D Bhuvana Suganthi, Manjunath R, Punitha A, Raghupathi.S

Abstract: ***This work is to overcome the data confidentiality issue and lack of security due to possibility of unstable connections, inflexibility in transmission rate in a distributed environment. This work is carried in three stages. Firstly, the secure path is identified based on energy, link quality, and delay towards the destination node. The quality of the link is considered due to the node mobility in the mobile network. Secondly, in the identified secured path, the next algorithm called Distributed Caching and Fault-tolerant Communication (DCFC) protocol is employed to monitor the failure occurring on routing tree and initiates failure recovery technique which is suitable for increasing the data transmission rate with very less failure Thirdly, Trusted Security Policy based Routing Algorithm (TSPRA) is implemented to overcome the packet drops and increased overhead due to lack of security which proves that data are well secured due to specific access control policies and increasing the high secured data size. Henceforth the level of security is increased with respect to reliability, recovery, confidentiality, and integrity. Reliability is proved based on the linking of all the possible positive factors of the distributed mobile communication in a single system. This performance leads to enhancement of productivity, personal safety and ability to protect their way to public service in terms of communication through wireless networks in a distributed environment***

Keywords: ***Mobile Distributed Networks, Trusted Security, Distributed Caching, Routing Algorithm, Overhead Ratio, Mobile Host, Reliable Paths, Bloom Filter, Mobile Agent.***

I. INTRODUCTION

The utmost impact on our regular lives is wireless communication among mobile devices. Heterogeneous devices which have been established using various routing networks require the suitable functionality in a distributed manner. In this environment, mobile networks routing takes more number of multiple hops and this is a major challenging task because of mobility node, peer to peer mode of communication, lack of predefined infrastructure, time, security, energy consumption and power. A major component in mobile network is security in communication for proper functioning with suitableprotocol [1]. The major issue in any distributed system is security.

Revised Manuscript Received on February 05, 2020.

* Correspondence Author

Dr. D Bhuvana Suganthi*, Department of Electronics and Communication Engineering, BNM Institute of Technology, Bengaluru, India. Email:bhuvanasuganthi@gmail.com

Dr. R. Manjunath*, Department of Electronics and Communication Engineering,AMCEC,Bengaluru, India. Email:manju_r_99@yahoo.com

Dr.Punitha A, Department of Electronics and Communication Engineering, Trichy Engineering College, Thiruchirapalli, India. Email:sweetpunitha@gmail.com

Raghupathi.S, Department of Electronics and Communication Engineering, IBRICT, OMAN Raghupathi.Senthilvel@ibrict.edu.om

Security mechanisms are used for safeguarding the system from intruders and to satisfy the requirements of the security applications. Integrity and availability schemes are concentrated in the distributed storage systems [2]. Security level is assigned to each transaction for a multilevel protection in a distributed database system. Hence the level of security is increased with respect to reliability, recovery, confidentiality and integrity.A source node uses either direct link or a multiple hop routing method for enhancing communication between two nodes. A high transmission range is possible in the multi hop method. Performance may behind in packet delivery to the nodes at destination due to node mobility. [2]. A research on routing protocol being done during the recent years in the area of mobile networks says that, on demand routing protocols is better compared to other routing algorithms in the presence of mobility of nodes in terms of routing overhead and packet delivery ratio. Battery powered mobile nodes with less capacity, affect various parameters like throughput, energy conservation and delay time in the network. Hence, an efficient energy based protocol is needed to enhance the duration of the node and network. The potential for significant increases in the accessibility of information technology is offered by distributed computing.

II. RELATED WORKS

In recent years, there are several studies on distributed caching, security in routing related parameters. The few work on caching technologies is given by [3]-[9] which provides distributed methods of dynamism and, mobility which has to be addressed with highly dynamical approaches. These methods provides different challenges such as efficient access to distributed data sources, communication failures, dynamic load balancing and lack of flexibility. Caching is a major role in mobile computing with its capability to improve the performance and availability limitations of weakly-connected and disconnected operation. But evaluating the other methods of planning to caching process for mobile computing is quite complex. The work based on fault tolerance is given by [10] – [17] which provide lack of security during routing leads to loss of packets and increase in overhead. The work on routing algorithm for mobile computing is given by [18] such as agreement routing algorithm to improve the performance factor in data transmission. The work on Mobile Agents is given by [19] which is used in this work for monitoring the failure nodes and algorithm to recover the failure nodes is implemented.

III. RESEARCH METHODOLOGY

A systematic study of existing routing protocols is done and simulated with dynamic network size. Three steps involved to implement this paper.

1. Identification of Secure Routing Path in Mobile Distribution Algorithm which computes the reliability of each of the neighbor nodes and picks a node in such a way that it has highest reliability and moves forward and repeats the process till reaching the destination to place the nodes randomly in the network.
2. Design of Distributed Caching and Fault Tolerant Communication on Secure Routing Path in Mobile Distribution Algorithm.
3. Design and implementation of Secure Policies on Fault Tolerant Communication on Secure Routing Path in Mobile Distribution algorithm.

Each step is explained below with the results obtained.

IV. RELIABLE SECURITY PATHS IN MOBILE COMPUTING

The major factor in mobile networks is to ensure the better network with suitable algorithm. In distributed mobile networks, there is a possibility of communication failures, unstable connection and lack of flexibility. In this environment, generally mobile networks routing take more number of hops arises from mobility of the nodes, peer-to peer mode of communication, lack of predefined infrastructure, time, power, security and energy consumption. The major challenging task is to address security and energy simultaneously. The reliable path which is suitable for strong link, less delay and energy in distributed environment is identified based on the shortest path algorithm. Hence there is increase in the level of security with respect to reliability, recovery, confidentiality and integrity. To identify the suitable path from all the possible nodes, this algorithm is implemented. Initially, a reliable path is established among the nodes on the basis of parameters link strength, delay and energy. The shortest path with best link strength, least delay and least energy consumption is determined [20]. The path taken by a source may not exist and there could be a lack of performance in packet delivery to the nodes of destination after a small interval of time as a result of node activity. The efficient path is calculated based on the product of the link quality and residual energy with respect to the delay. The path which has the high secured mechanism is considered as the most reliable path.

$$Secure\ Path = \frac{Link\ strength * Residual\ Energy}{Delay} \quad (1)$$

The calculation is based on energy, estimated link quality, and delay towards the destination node. Estimating the delay and energy is not up to the requirement to identify the data transmission without congestions from one end to the other end. The link strength status is identified by a physical layer and its information is passed on the upper layer which indicates a smaller link eminent zone [21]. The signal strength is weaker in this region, leading to link failure. Hence the low signal strength link is discarded from the selection of route. The node which has a higher link quality is considered as the best link strength. For more than one node has the same link quality, the secured path is calculated on the basis of smaller delay and energy consumption. Equation 1 is not considered in the noise occurred in the path, since the wavelength carrier removes the noise. Among all the paths available, the path which has a high link strength and known for less duration for transmission of data is calculated. If, the link strength is not up to the level, next path is calculated despite the duration being high. Hence the formula proves the equality of the secured path to link strength with less residual energy and delay. This is experimented between two nodes among 15 numbers of nodes. The nodes assumed for communication is node 4 and node 12. Fig.1 to Fig. 4 shows the various identified reliable paths Fig. 5 is identified as the best reliable path based on the link strength, residual energy and delay.

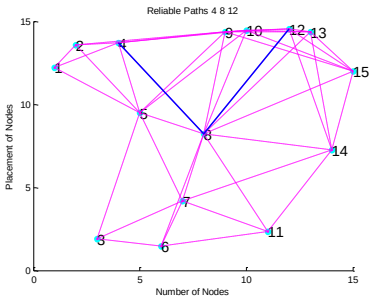

Fig. 1. Secured path between node 4 and node 12 via node 8

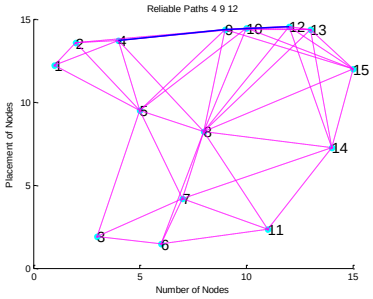

Fig. 2. Secured paths between Node 4 and Node 12 via Node 9

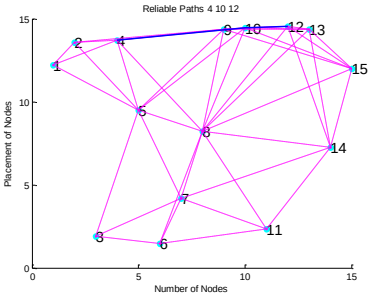

Fig.3.Secured paths between Node 4 and Node 12 via Node 10

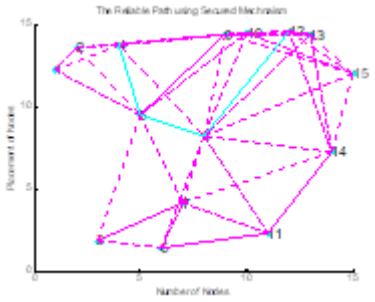

Fig. 4. Secured paths between Node 4 and Nnode 12 via Node 5 and Node 8

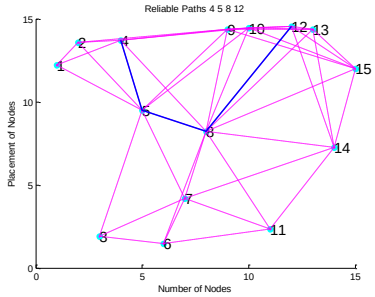

Fig. 5. The Most secured path between Node 4 and Node 12 through node 5 and Node 8 based on Secured Mechanism

TABLE-I: Performance Comparison of different Secured Path between Node 4 to Node 12

Secured path	Quality link	Duration	Energy level
4 – 8 - 12	0.0172	1.0397	1.9269
4 – 9 - 12	0.0247	0.9026	1.8348
4 – 10 - 12	0.0811	0.9219	1.9089
4 – 5 – 8 - 12	0.1052	1.4467	2.8189

The node which has a higher more link quality is considered as the best link strength. It is implemented using MATLAB. From the table I, the most reliable path is based on the maximum value of secured mechanism is 4 – 5 – 8 - 12.. All possible reliable paths are calculated based on the time, cost, and energy consumption. The results obtained shows that delay and link strength is up to the level, more consumption of energy. In other path, energy consumption and time is less but weak link. Therefore the same set of reliable communication is implemented in DCFC technique and the same is simulated in Ns-2 to improvise the routing strategy in single implementation method.

V. DISTRIBUTED CACHING AND FAULT TOLERANT COMMUNICATION (DCFC)

Caching technique is added to improve the routing strategy in the distributed network following the identification of the reliable path. Evaluation of various caching plans for mobile computing is always difficult. Each mobile host is deployed by a distributed mobile agent within the reliable route for detecting faults. Mobile Agent plays a major role in this algorithm, with initial monitoring of the failures occurring in the routing tree [22]. Mechanism to recover the failure is initiated, if a mobile host detects, the failure of its immediate level nodes. Based on game theory with proper selection of caching policy, the content distribution is performed Simulation results are used for showing the enhancement of the reliability of the proposed technique DCFC and for reducing communication failure.

A. Failure Monitoring Algorithm

The Mobile Agent monitors the failures of the tree members. Fig. 6 shows the failure monitoring by the mobile agents. The notations used are

MA_i	Mobile agent
MH_i	Mobile host
AACK	Active acknowledgement message
aack_timer	Timer for receiving AACK
AC	Active message

1. Begin
2. MAi periodically transmits AC to MHi
3. If MHi receives AC from MAi, then
4. MHi send AACK to MAi
5. 5. End if
6. If aack_timer expires , then
7. MHi is about to fail, if MAi not receives AACK from MHi,
8. End if
9. New mobile agent MAnew.is generated by MHi.
10. Monitoring task is initiated by MAnew
11. If MHi is about to fail , then
12. MAnew is shifted to other trusted MHi
13. End if
14. If MHi detects failure of MHi+1, then
15. Initiates failure recovery technique
16. End if
17. End

Each MA_i regularly transmits the Active message shortly called as AC message to its $MH_{i,t}$ to be aware of failed or

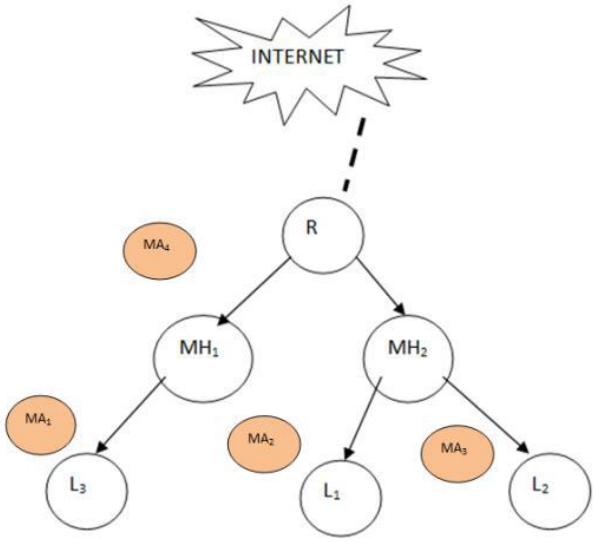

Fig. 6. Monitoring the Network Failure

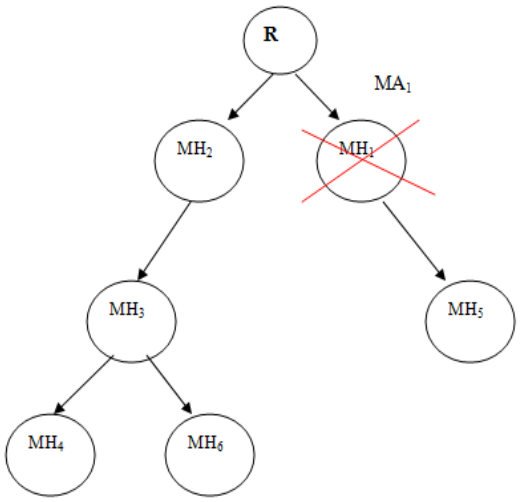

Fig. 7. MH1 fails

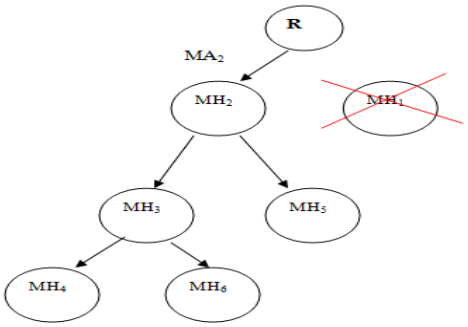

Fig. 8. New MA at MH2 recovers MH1

active by a mobile agent. Every interval with pre-defined time, mobile agent decrements the parameter, 't' for its immediate lower level nodes. Based on receiving AC message from i^{th} Mobile Agent, Active Acknowledge (AACK) message is sent by MA_i. If AACK message is not received by MA_i, monitoring of the immediate next lower level nodes is generated to perform effectively if needed. Monitoring of the task is initiated by the new mobile agent (MA_{new}) and all the nodes are informed about its location. When the current MH_i is tend to fail or not able to communicate, it itself moves its MA_i to other secured MH_j, from that the task is monitored by MA_i. The trusted MH is selected based on its previous failure history. The MH with least number of failure counts is assumed to be trusted. Technique to recover failure is initiated. This method of failure monitoring, results in the absence of failure and low overhead.

B. Technique of Failure Recovery

Failure recovery technique is initiated, if immediate level nodes have failed [8]. The recovery process is taken based on the capability and availability of nodes. This process takes place in three various situations.

1. Chooses a new node and generates new MA which performs the same task as before. Fig.7 show a failure in MH1 is detected. Then a new mobile agent MA2 is created and deployed in MH2 which then takes over the job of MH1 as illustrated in Fig. 8.The child MH5 of failed MH1 is then connected to MH2.
2. If failure node is at immediate lower level then replacing the failed one is available as follows.
    - Mobile Host checks its lower level nodes, is there any suitable node for replacement.
    - It is allowed to take over the role of failed MH, if any node exists.
    - The updates about the location and its replacement are informed to all the nodes in the path between the failed node and the Mobile Host.

Fig. 9 shows MH_3 fails which there is a failure of an immediate lower level node of MH_2. In Fig. 10, MH_2 designates MH_4 which is the child of MH_3 to recover the job. It then informs the other child MH_6 to connect to MH_4.

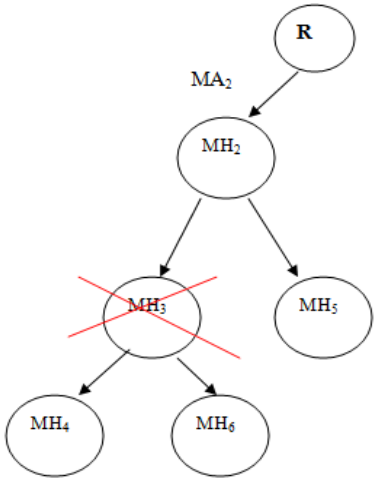

Fig. 9. MH3 fails

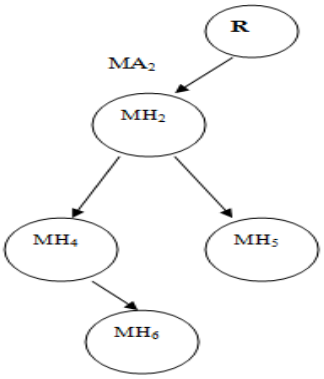

Fig.10. MH4 recovers the job of MH3

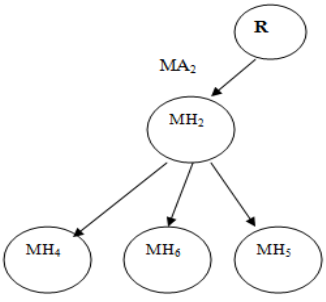

Fig. 11. MH2 recovers the job of MH3

Fig. 11 shows that MH_2 does not have the ability to designate MH_4 to recover the job of MH_3 as shown in Figure 10, then it designates itself as the recovery node of MH_3 and inform the children MH_4 and MH_6 to connect with it.

3. If no lower level nodes available or no new node for node replacement of failed node, then
   - The immediate higher level node is recommended by MH to take the role of failed node.
   - All the available nodes in the path are informed by the new node about its location and its replacement.

C. Game theory based selection of Caching policy

The mobile nodes pre-fetch the data when it is received from the internet, share and

store the information. The procedures involved in this approach are presented in the following algorithm. The notations used are

n_i	Any MH in the system
P	public cache
x_i	most downloaded websites
Q	node has possibility to download a set of all websites
CP {ni, nj,}	Caching Policy
UF_{ni}	utility function for n_i
$\{n_i, n_j\}$	neighboring nodes.

While selecting caching policy, to improve the total expected utility of nodes is also executed. The utility function (UF_{ni}) is used to select the caching policy (CP) of n_i for the website Q at time t. When any copy of the website is retrieved, a request from Q can be satisfied. This process can be possible only during following situations such as the when the websites are not updated often and quick diffusing of content among users that cache it. A feasibility condition is defined if the request is raised by the node for a website during time slot. This inequality proves that the node request is satisfied. Here $CP_{n,q} = 1$ reveals that the node keeps the needed website in its public cache. The condition will be satisfied during the situations when n_i meets n_j.

As per the parameters delivery Ratio, throughput, packet drop, and overhead ratio, evaluates the performance of the new algorithm. This content based distribution is performed with related to game theory of caching policy. The results prove that the proposed technique improves the security level by reducing the average packet drop and delay involved in identifying and recovering from failures. In presence of increased mobile hosts and cache sizes, the proposed DCFC has 24% and 16% reduced packet drops, respectively, when compared to existing RMP technique. Similarly, it attains 29% and 18% reduces delay when the mobile hosts and cache sizes are increased [23].

VI. TRUSTED SECURITY POLICY AND ROUTING ALGORITHM (TSPRA)

This proposed algorithm implemented the concept as, full access control is assigned to the mobile host (MH) with least access control and maximum reputation value is assigned to MHs with least reputation value which is offered by a technique of mobile agent monitoring. To reduce storage overhead, bloom filters are used to store the access control policy. For data transmission, agreement routing process is used as routers to forward the data based on the nodes with maximum availability function and access control [22]. The results shown in simulation that provides better in security while reduction of overhead in storage and in packet drops.

A. Access Policy

Access Control Policy (ACP) is available in every mobile host for which consists of the following access permissions. Forward (F), Process (P), Read (R) and Modify (M).Any particular combinations of permissions, Mobile Host may possess an ACP with A MH with RMFP permissions possess full access control, who belongs to the top or administrator level.

B. Bloom Filter

Bloom filter (Q) is used for the need of large amount of memory required by the amount of source data. It has better advantage in space compared to the other data structures for representing sets. Hash functions are computed over the element to fit a data element w into z.

Z is inserted into the filter by setting the bits $H_i(z)$ to one. On other hand, c is assumed to be member of Y if any bits $H_i(z)$ are set and guaranteed not to be member if any bit $H_i(z)$ is not set. Utilization of memory is effectively managed and storage overhead is reduced by this technique.

C. Cumulative Reputation Value Estimation

Residing of mobile agent with each MH is calculated based on attempts to honest make by the MH. Level of honesty is evaluated with respect to MH performs the recommendations from others MAs are obtained. Then each MH is assigned with cumulative reputation value (CRV) which is a combination of the recommendations from other MHs and its direct interaction with MHs.

D. Honesty

The trust obtained by MH_i and its nearby node MH_j is honest after the observations towards MH_j are termed as Honesty ($T_{ij}^{H}(t)$). Based on monitoring the access permissions (AP_i), level of honesty is calculated by MH_i Where, $hon_j(i)$ represents the honesty level of MH_j which the MA has noted at interval t. It depends on the parameters such as number of packets that are successfully received and number of packets that are forwarded to the gateway. MH_j is dishonest for low AP_i. MH_j is partly honest for medium AP_i, MH_j is honest for AP_i is high.

E. Trusted Security Policy

Each host in the mobile multicast tree (MH) is deployed with an agent of distributed mobile nodes (MA). It executes the following process:

- If the number of attempts to the honest level (MH), the interactions with other MHs are evaluated directly.

- Based on interactions, the recommendations from others MAs are obtained similarly.
- Each MH is assigned with cumulative reputation value (CRV) which is a combination of the recommendations from other MHs and its direct interaction with MHs.

VII. RESULTS AND DISCUSSIONS

A. Impact of network size on attackers

The performance is analyzed between DCFC and TSPRA based on variable number of nodes from 21 to 53, Table 3 shows the analysis between DCFC and TSPRA of variable number of nodes for fixed attacker size as 2 and cache size as 50kb. The results prove that TSPRA outperforms better in performance metrics than DCFC .In this case, the node size is varied from 21 to 53 keeping the size of attackers as 2 and cache size 50Kb. Fig.12 to 15 illustrates the delay, packet drop, throughput and packet delivery ratio of both TSPRA, compared with the DCFC
technique. Simulation results show that TSPRA has 43% reduced delay, 49% lesser drop, 27% higher throughput and 32% higher delivery ratio when compared to DCFC, in presence of increased number of attackers as 2 and cache size as 50Kb.

Table –II: Performance comparison of variable nodes with attacker 2 and cache size 50kb

Attacker-2,Cache Size-50								
Number of Nodes	Delay		Drop		Throughput		Delivery Ratio	
	DCFC	TSPRA	DCFC	TSPRA	DCFC	TSPRA	DCFC	TSPRA
21	3.799	3.747	2593	2594	5816	6085	0.68	0.696
29	5.665	3.344	6104	3328	7489	10644	0.54	0.759
37	5.818	3.714	7004	3874	8707	11362	0.55	0.740
45	7.755	2.685	1186	2841	7266	11535	0.38	0.798
53	8.785	2.685	1209	2841	7143	11535	0.37	0.798

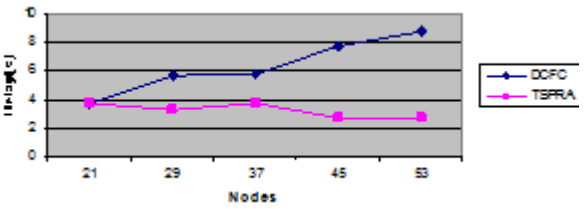

Fig.12. Variable Nodes with Delay(Attacker 2, Cache Size50kb)

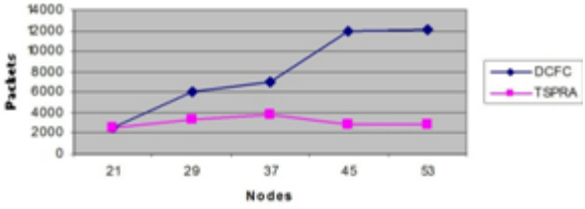

Fig.13. Variable Nodes with Drop (Attacker 2, Cache Size 50kb)

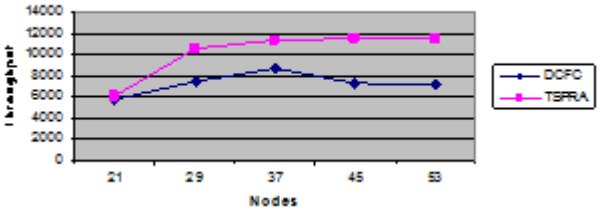

Fig.14. Variable Nodes with Throughput (Attacker 2, Cache Size 50kb)

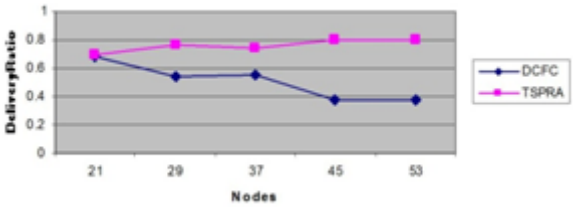

Fig. 15. Variable Nodes with Delivery Ratio (Attacker 2, Cache Size 50kb)

B. Impact of Cache size on Attackers

The performance is analyzed between DCFC and TSPRA based on variable cache size from 50kb to 250kb.Table IV shows the analysis between DCFC and TSPRA of variable cache size fixed attacker size as 2 and node size as 53. The results prove that TSPRA outperforms better in performance metrics than DCFC. In this case, the cache size is varied from 50 to 250Kb by assigning the number of nodes as 53 and attackers as 2. Figure 16 to 19 illustrates all the performance metrics for both proposed DCFC and TSPRA techniques. Fig. 16 to 19, the proposed TSPRA is compared with the DCFC technique. Simulation results show that TSPRA has 69% reduced delay, 77% lesser drop, 42% higher throughput and 58% higher delivery ratio when compared to DCFC, by keeping number of attackers as 2 and number of nodes as 53.

Table-IV: Performance comparison of variable cache size with attacker 2 and 53 nodes

Attacker-2, Nodes-53								
Cache Size	Delay		Drop		Throughput		Delivery Ratio	
	DCFC	TSPRA	DCFC	TSPRA	DCFC	TSPRA	DCFC	TSPRA
50	8.785	2.3364	12090	2627	7143	11735	0.375	0.813
100	8.612	2.5996	13786	3162	7683	13032	0.36	0.803
150	8.5	2.3739	16966	3435	7737	15059	0.32	0.811
200	8.142	2.5996	19098	7211	9428	13032	0.33	0.803
250	9.318	3.5941	25647	3162	8775	18716	0.26	0.72

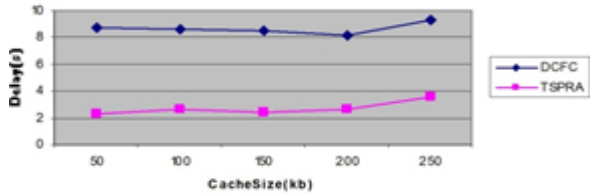

Fig. 16. Variable Cache Size with Delay (Attacker 2, 53 Nodes)

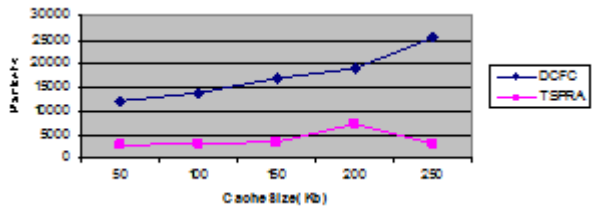

Fig. 17. Variable Cache Size with Drop (Attacker 2, 53 Nodes)

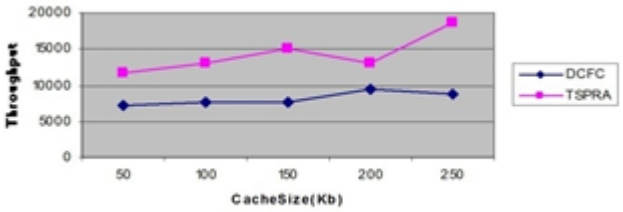

Fig. 18. Variable Cache Size with Throughput (Attacker 2, 53 Nodes)

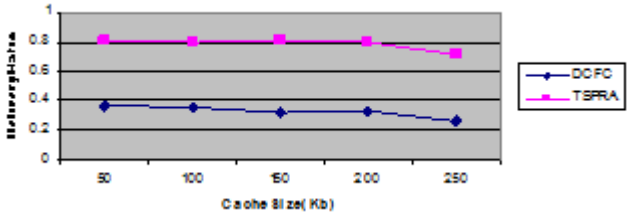

Fig. 19. Variable Cache Size with Delivery Ratio (Attacker 2, 53 Nodes)

VIII. CONCLUSIONS

This work identified the secured path based on link quality and implemented the failure recovery technique in the path and finally the data path is not affected for variable attackers and variable nodes. The high performance in TSPRA leads to enhancement of productivity, personal safety and ability to protect their way to public service in terms of communication through wireless networks is implemented in a distributed environment. Even a faster way of communication and unfailingly is reliable due to adaptable features in this method. These performance factors proved that the improvement in security with high memory capacity, less delay, less overhead ratio and overall increase in network lifetime of wireless sensor network. If the cache size is improved, the performance is affected to some extent. This has to be considering for the further work.

FUTURE WORKS

Mobile distributed networks with cloud computing has an attention received recently for the future work. Cloud computing technology integrates the heterogeneous storage devices through diverse functions such as distributed file systems and provides facilities of data storage and service functions. Cloud computing has number of advantages includes reduction in energy consumption, memory capacity and overhead ratio. However, bandwidth and the security constraints becomes a hold up in this centralized processing architecture. Hence in future, this work may be moved in the direction of extending the presented solutions to mobile cloud environment.

REFERENCES

1. Hiroyuki kasi, “Embedded Middleware and software development kit for area based distributed mobile cache Systems”, IEEE, 2013.
2. D. BhuvanaSuganthi, “High Performance Mobile Computing Nodes in Distributed Networks”, Volume 4, Issue 3, March 2014,www.ijarcsse.com
3. PietroMarchetta, Jaime Llorca, Antonia M. Tulino, Antonio Pescap´e, “MC3: A Cloud Caching Strategy for Next Generation Virtual Content Distribution Networks”,IEEE, IFIP Networking, ISBN: 978-3-9018-8283-8, pp:332-340,2016.
4. Jesper Pedersen, AlexandreGraell i Amat, IrynaAndriyanova and Fredrik Brannstrom, "Distributed Storage in Mobile Wireless Networks with Device-to-Device Communication",IEEE,2016
5. SemBorst, Varun Gupta, Anwar Walid, “Distributed Caching Algorithms for Content Distribution Networks”, IEEE INFOCOM 2010 proceedings, 2010.
6. Brian L. Tierney, Jason Lee, Brian Crowley, Mason Holding, “A Network-Aware Distributed Storage Cache for Data Intensive Environments”. Proceedings. The Eighth International Symposium on High Performance Distributed Computing (Cat. No.99TH8469), pp: 185 - 193, 1999.
7. NehaPathak and Dinesh Chandra Jain, “Performance of Cache in Distributed Systems”, Volume 2, Issue 5, May 2012, International Journal of Advanced Research in Computer Science and Software Engineering.
8. Stratis Ioannidis, Laurent Massoulie and AugustinChaintreau, “Distributed Caching over Heterogeneous Mobile Networks”, ACM SIGMETRICS PerformanceEvaluation Review, Vol. 38, No. 1, ACM, 2010.
9. Huayong Wang and Li-ShiuanPeh, “MobiStreams: A Reliable Distributed Stream Processing System for Mobile Devices”, Parallel and Distributed Processing Symposium, 2014 IEEE 28th International, 2014.
10. Jon B. Weissman and David Womack, “Fault Tolerant Scheduling in Distributed Networks”. UTSA Technical Report, CS-96-10, October 1996.
11. A. Baratloo, P. Dasgupta, and Z.M. Kedem, “Calypso: A novel Software System for Fault-Tolerant Parallel Processing on Distributed Platforms,” Proceedings of the fourth IEEE International Symposium on High Performance Distributed Computing, ISSN:1082-8907,1995.
12. HarpreetKaur, UsvirKaur, "A Review on Mobility in Distributed System", IJCST Vol. 7, Issue 2, April - June 2016.
13. K. Birman, “The Process Group Approach to Reliable Distributed Computing”,DARPA/NASA grant NAG 2-593 and by grants from IBM, HP, Siemens, GTE and Hitachi, 1992.
14. G. Popek , B. Walker , J. Chow , D. Edwards , C. Kline , G. Rudisin and G. Thiel, "Locus: A Network Transparent, High Reliability Distributed System", Proceedings of the 8th ACM Symposium on Operating Systems Principles, pp. 169-177, 1981
15. Birman, K. and Cooper, R. The ISIS project: Real experience with a fault tolerant programming system. European SIGOPS Workshop, Sept. 1990. To be published in Oper. Syst. Rev. (Apr. 1991). Also, available as Cornell University Computer Science Department Tech. Rep. TR90-1138.
16. Seyed Ali Mohammad Javadian and Maryam Massaeli, “A fault location method in distribution networks including DG”, Indian Journal of Science and Technology Vol.4 No. 11 (Nov 2011).
17. Meshal A, Al-shaher A, Manar M, Sabry B, Ahmad S, and Saleh S (2003) Fault location in multi-ring distribution network using artificial neural network.” ElectricPower Sys. Res. 64, 87–92.
18. DamianosGavalas, George E. Tsekouras, Christos Anagnostopoulos, “A mobile agent platform for distributed network and systems management”, the Journal of Systems and Software 82 (2009) 355–371.
19. Arles Rodrıguez, Jonatan Gomez and Ada Diaconescu, "Towards Failure-Resistant Mobile Distributed Systems Inspired by Swarm Intelligence and Trophallaxis", Proceedings of the European Conference on Artificial Life 2015, pp. 448-455.

20. Subramanian Ganesh and RamachandranAmutha, “Efficient and Secure Routing Protocol for Wireless Sensor Networks through SNR Based Dynamic Clustering Mechanisms”, Journal of Communications And Networks, Vol. 15, No. 4, August 2013.
21. D. BhuvanaSuganthi, “Fault Tolerance Communication in Mobile Distributed Networks”, International Conference on Data Engineering and CommunicationTechnology, Springer Series, August 2016.
22. D. BhuvanaSuganthi, “Reliable Security Policy in Mobile Distributed Network”,IEEE International Conference on Recent Trends in Electronics, Information and Communication Technology(RTEICT), IEEE Communication Society, IEEE Digital Library, May 2016.
23. D.BhuvanaSuganthi, “,“Efficient Data Fetching with Supportive Caching in Mobile Distributed Networks”, International Journal of Engineering Trends and Technology, Volume 59, Issue 3, May 2018.

AUTHORS PROFILE

Dr. Bhuvana Suganthi D, (Bhuvana Suganthi Dharmaraj) Associate professor, in the department of Electronics and Communication Engineering at BNM Institute of Technology, Bengaluru. She received the Bachelor’s degree in Electronics engineering from Bharathidasan University in 2002, Master’s degree in embedded system technologies from Anna University in 2008, and Ph.d from Visveraraya Technological University, Karnataka in 2018. She has 16 years of teaching experience. She has 10 publications in National, International Conferences and 4 International Journals. She is a member of ISTE AND IEI. Her research interests include wireless sensor networks, distributed computing, Digital Technologies.

Dr. Manjunath R (Manjunath Ramachandra), Professor in the Department of Electronics and Communication Engineering, Bengaluru. He received Bachelors degree, Masters degree and Ph.d degree in Electronics engineering from Bangalore university. He has blend of industry & academic experience for 18 years in the overlapping verticals of Signal processing including Information management, web technologies, media & entertainment, Wireless/mobile and networking. Research in the same field led to PhD, about more than 85 international publications and a book.

Dr. A.Punitha (ArockiasamyPunitha) Associate Professor in the Department of Electronics and Communication Engineering at M.NM Jain Engineering College, Chennai. She acquired her Bachelor’s degree in Electronics and Communication Engineering from Bharathidasan University, Tiruchirapalli in 2002. She obtained her Master’s degree in Communication Engineering from Anna University, Chennai in 2009 and Ph.D degree from Anna University, Chennai. She has over 15 years of experience in teaching and guiding projects. Her areas of interests include Vehicular Ad hoc Networks, Wireless Sensor Networks, Digital Communication, Optical Communication and Network Security.

S.Raghupathi (Senthilvel Raghupathi) obtained his Bachelor’s degree in Electronics and Communication Engineering from Bharathidasan University, Tiruchirapalli in 2002. Then he obtained his Master degree in VLSI Design from SASTRA University, Tanjore. Currently, he is serving as a Lecturer in Department of Engineering, at IBRI College of Technology,Oman. His specializations include VLSI design, Communication Engineering, and Networking. His current research interests are Public Key Infrastructure, Network Security and Authentication Server and VANET’s.