International Journal of Scientific Research & Engineering Trends
Volume 3, Issue 5, Sept.-2017, ISSN (Online): 2395-566X

# Secret Sharing Schemes over MANET to Avoid Cheater Participation

**Nisha Bharti**
M.Tech Scholar, RITS Bhopal M.P.,
Email: nnishabharti@gmail.com

**Hansa Acharya**
Asst. Prof., Dept. of CSE RITS Bhopal M.P.
Email: hansaacharya@gmail.com

***Abstract* – Mobile Adhoc Networks (MANET) has become the most important means of communication in our day to day life. A rapid advance in technology and proliferation of wireless devices in the recent times has attracted huge attention towards research on MANET. Secret sharing is an important phenomenon in order to secure the data transmission over MANET. There are number of approaches have been proposed in the current scenario. Recently various algorithms have been proposed in this regards. But there is problem of wrong reconstruction due to fake player participation. To overcome this problem this work presents an optimal approach for secret sharing. There is some problem that may occur while reconstructing the data at the reconstruction site. In this manner this dissertation has been proposing an optimal approach in order to perform secret sharing. In this paper initially proposed methodology use secret building phase, initially data packet MP can be divided into number of neighbor node and attach CRC value of rest with each phase for authentication at destination. Proposed Methodology used to calculate combine CRC for N-1 phase for any random phase. Whereas at destination end for each datagram CRC value is use to verify cheater participation. If CRC is not match then destination node send retransmission request to sender and whole process freshly repeated.**

***Keywords* – Mobile Adhoc Networks, Secret Sharing, Secret Building Phase, Secure Communication.**

## I. INTRODUCTION

A Mobile Ad-Hoc network (MANET) is an infrastructure- less network of wireless mobile devices connected by wireless links that forms a temporary network. Every mobile device/node in MANET [1][2] is free to move randomly. Hence the topology of MANET also changes dynamically. Every mobile node can communicate with each other when found within the communication range of each other. MANET is also called multi-hop wireless network. MANETs have become one of the inevitable parts in our daily communication systems. It has also become very suitable means of communication during emergency cases such as rescue operations where there is a need to build temporary wireless application without infrastructure. There has been considerable demand for reliable communication due to the technological innovations in recent times. Hence, reliability of MANET has become an important area of research today.

An increasing dependence on more reliable services implies that there is a need to incorporate reliability analysis as an integral part in their planning, design and operation of systems. A system is highly reliable i.e. mostly available, if there is a negligible probability that the system will be down at any instant of time of usage. MANET reliability is an important benchmark for reliable communication. The qualitative definition of network reliability is the ability of the network to continue services in the case of component failures [3]. The quantitative definition of network reliability is the probability of existence of at least one path between a specified numbers of k-nodes under known conditions [4]. Therefore, network reliability of MANET must focus on communication. The progression communication of MANET is fragile compared to wire network due to some of its attributes such as dynamic topology, environment without infrastructure, multi-hop routing, node mobility, rapid deployment, constrained resource, flexibility, self-organizing, specific application, MANET types i.e. homogenous or heterogeneous etc. Most of these attributes affect the continuity of network connectivity and hence they are important for measuring the network reliability of MANET. Reliability analysis may refer to two-terminal, k-terminal and all-terminal reliabilities of a traditional network where each node is considered as a terminal. The successful communication between a pair of nodes is defined as the presence of one or more operating paths between the nodes. The probability of successful communication between two nodes of the network is called two-terminal reliability [4][6]. It is the probability of successful transmission of a message from source node to destination node. The probability of successful communication between a node and all other nodes of the network is called all-terminal reliability i.e. the probability that node ni can communicate with node nj for all pairs ninj where $i \neq j$. The k-terminal reliability is the probability that a subset of k nodes are connected where $2 \leq k \leq n$. The metric that will give the probability that the operating nodes can successfully communicate is the all-operating terminal reliability [7]. This is useful for reliability analysis of nodes that are disconnected due to lack of communication links rather than disconnection as a result of radio failure.

Most reliability analysis is focused on all-terminal reliability. This is true for MANET because based on this analysis, protocol design and complex MANET deployment can be guided. The methods used for traditional infrastructure based networked systems i.e. enumeration, transformation, reduction, decomposition,

factoring theorem etc. cannot be used directly for analysis/computing the reliability of MANET. This is because we must consider node reliability, link reliability and node mobility model (that gives rise to dynamic topology having many configurations) for computing all terminal reliability of MANET [7][8]. Additionally, network congestion is more serious in MANET compared to that of traditional networks because of multi-hop channel routing and node mobility. This will lead to dropping of packets and will affect all terminal reliability of MANET.

## II. Secret Sharing

The basic idea of secret sharing [19, 20, 21, 22] is to divide information into several pieces such that certain subsets of these pieces (shares) can be used to recover the information. Fake players want to retrieve several shared information, in order to make participate in reconstruction of secret information and try to destroy the information.Secret sharing scheme [19, 20, 21, 22] having three different phases namely share building phase, share

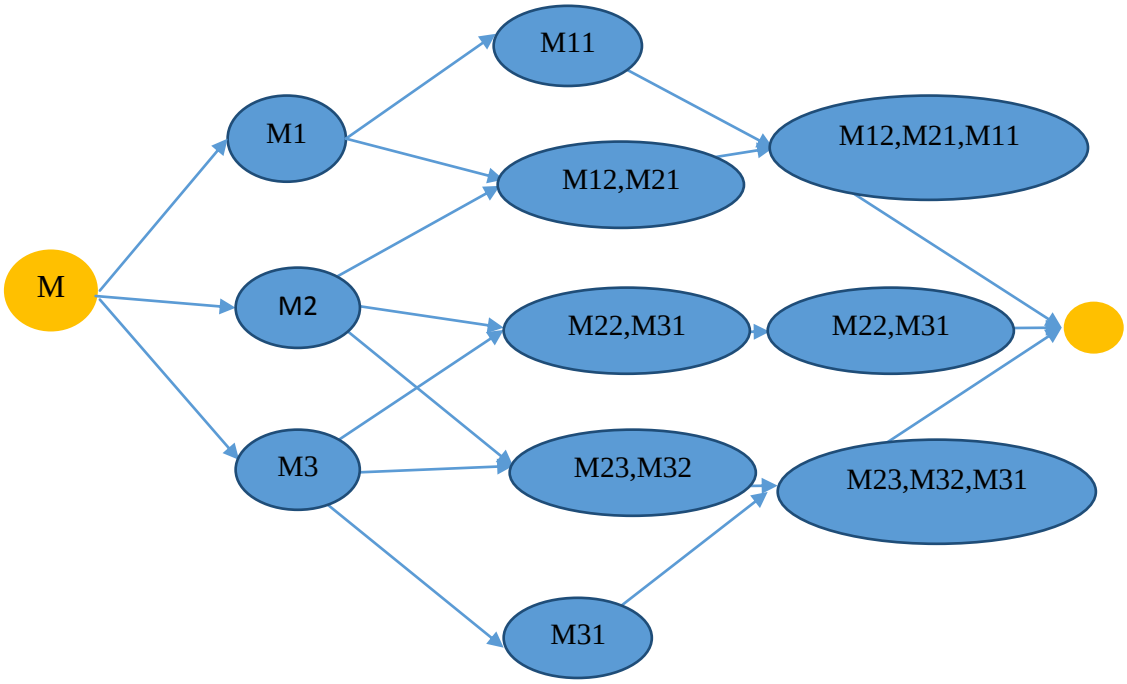


Fig.1. Share Building and Distribution Phase

distribution phase and secret reconstruction phase. Share building phase used to select share holder as neighbor node from list of neighbor table. Share distribution phase used to distribute each sub message to each and every qualify neighbour as show in share distribution phase of figure 1. Share building phase distribute all N different data packet, then share recovery phase combine any random T phase to reconstruct original message image.

The method [24,25] used so far requires all shared images for recovery. In real application, if recovery is possible using some shared images then it can save the time and also stop fake player participation. In this paper, a Secret sharing method is proposed which is based on threshold value. A secret image is divided into N sub-images and by combining any T sub-images, the original image is recovered without error. Here T<<<N.

With rapid growth of computers and computer networks, enormous amount of digital data can easily be transmitted or stored over network. However, the intruders can easily sense or manipulate the confidential data transmitted over the networks by some cryptographic tools. So recently numerous of research has been carried in the field of information security and number of researcher work in the field of efficient secret sharing scheme.

## III. Related Work

A Mobile Ad-hoc Network (MANET) has been studied in order to realize a ubiquitous society. However, MANET has many issues. One of the issues is security. This section evaluates different research that has been carried out in MANET security field till now. One of the paper present secure communication method using secret sharing scheme over MANET by adding dummy packet transmission and storing multiple shares in a single packet. And also the improvement achieves packet reduction that results in energy saving and collision reduction. But still needed to realize more improvement in reach ability of secure communication and to clarify how to decrease the number of non-member nodes that are capable of restoring a secret information[9].Another paper addressed two-terminal reliability computation for radio-

broadcast networks with the condition of failure of nodes only. However, they have not provided any relation between link failure probability and relative motion of the nodes [10].One of the method is used to optimize network reliability, network diameter and distance using genetic algorithm [11]. Another work proposed a heuristic approach for communication networks towards solving topological reliability allocation problems. The aim was to apply the heuristic approach for reducing the NP-hard problem for networks having large search spaces [12].some of them provided the review of the effect of mobility models on the life span of communication path existence in MANET[13].Paper[14] has presented an algorithm to determine the optimal distribution of elements within the network infrastructure to provide the highest terminal reliability. This algorithm is used for allocation ofmulti-state elements in communication networks[14] .Here they have used genetic optimizer to optimize the geographic layout of nodes in indoor wireless networks that may be used to extend local area networks[15].This work describes the effect of mobility on the bit error rate (BER) and minimum node spatial density of an ad-hoc network for obtaining full connectivity. They used BER as the network performance metric. However, the chances of node failure while accounting for total network connectivity were not considered[16].Ye proposed a node deployment strategy to increase the probability of a reliable path. This was achieved by placing nodes at strategic locations and possibility of practically controlling node mobility and limiting its use to such instances [17].This paper provides review of the situation where the nodes have an exponentially distributed finite lifetime between source and destination[18].Some authors have provided comparisons of various machine learning techniques to develop approximate reliability expressions for capacitated networks[19]. Some of them proposed methods to address both multi-state and capacitated network reliability. They provide multiple methods of addressing the reliability allocation optimization problems in the presence of common cause failures[20].Here an approach to incorporate uncertainty into reliability calculations by using Monte Carlo simulation and genetic algorithm has been proposed[21].This work described the process of mobile cell phone transition from one tower to another. They used Markov model to represent the network configuration change as one cell phone moves from one coverage area of one tower to the other area covered by another tower. They expressed network reliability as a function of the reliability of each node active in that configuration and the percentage of time that each configuration exists. This is not applicable to MANET since mobility of the nodes is not modeled. They assumed that failure of any active node in the path of a message results in failure which shows that configuration is a series system. This assumption is not suitable for MANET as extra paths may be found in between source and destination nodes[22]. In this paper they have derived a symbolic two-terminal reliability expression for MANET that can handle imperfect nodes in the dynamic network connectivity. They have focused on reliability of node and link for static topologies and presented the effect of the rate of node failure and mobility pattern on the two-terminal reliability of MANET[23].P. Brooks have analyzed mobile sensormulti-hop networks using a combination of percolation theory, random graph theory and linear algebra. They used a probabilistic adjacency matrix to analyze the network connectivity.However, they have not addressed the mobility of mobile nodes [24].Cook, Jason L have provided the analytical concepts of Adhoc networks along with Monte Carlo simulation to determine the two-terminal reliability of MANET. They considered the existence of a communication link as a probabilistic event with respect to the status of network nodes[25].Here they have provided the method using Monte Carlo simulation to determine the two-terminalreliability of MANET by addressing mobility of nodes, considering the existence of a communication link as a probabilistic event with respect to the status of network nodes. The reliability estimate comes out to be conservative which may not be practical for large MANET [26].S. Another author have shown the theoretical use of logistic regression method to compute the reliability of wireless sensor networks and other parameters[27].Some illustrated the effects of network size, transmission range and network coverage area on the reliability measures by modeling MANET as geometric random graph. They applied a Monte Carlo simulation to evaluate reliability of MANET whose node failure is governed by a known statistical distribution where links between the nodes are established dynamically depending on the transmission range of nodes. They emphasized on the influence of scenario metrics on the MANET reliability[28].This work have presented a novel two-terminal reliability analysis for MANET by proposing an effective Monte Carlo method[29] . They analyzed node mobility effect and node reliability on a real MANET platform. They have proposed a method to compute the reliability of MANET using logistic regression and they provided simulation results to support the correctness of their method[30]. In this paper, they study how to enhance the security of the original proposal and propose an improvement by which restoring the secret by malicious user is very hard to be executed. They evaluate the improved method from the view points of difficulty in restoration of key shares and show its effectiveness[33].

The basic idea of secret sharing is to divide information into several pieces such that certain subsets of these pieces (shares) can be used to recover the information. Where face player want to retrieve several shared information. In order to make participate in reconstruction of secret information and try to destroy the information. The main problem of existing approach is use all the participant to reconstruct the secret massage which take large time and detain the confidentiality of massage and as it required the entire participant at the time of reconstruction so if anyone

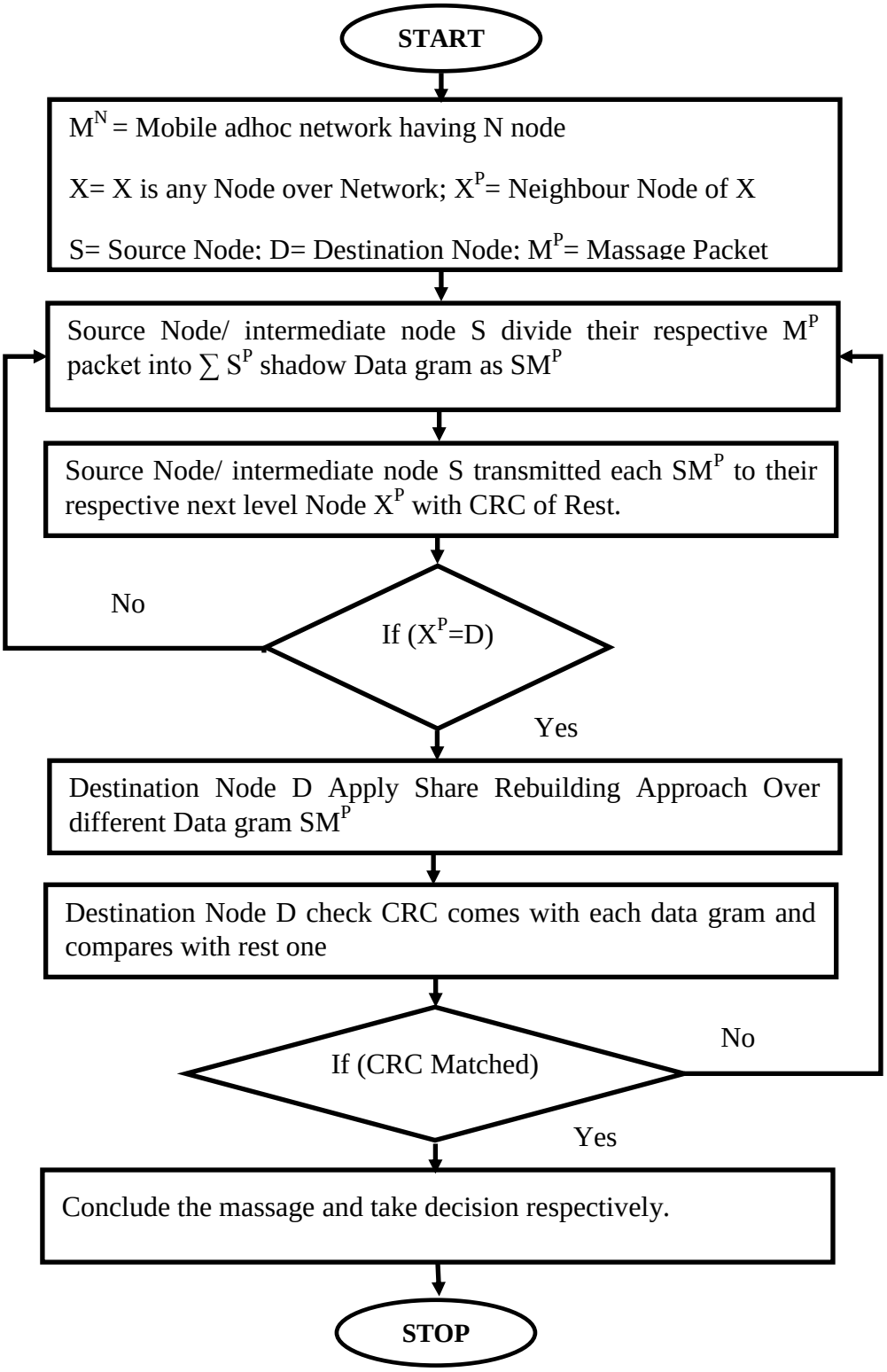


Fig.2. Proposed Methodology for Secret Sharing

is affected lead wrong reconstruction. So the main aim to randomize the number of participant required to reconstruct the secret massage, which leads higher level of confidentiality.

In Figure 2 $M^N$ denotes Mobile adhoc network having N node. X= X is any Node over Network; $X^P$= Neighbour Node of X

S= Source Node; D= Destination Node; $M^P$= Massage Packet

## IV. PROPOSED METHODOLOGY

In this paper proposed methodology use to split massage equal to number of neighbor node that the sender have and in order to achieve this goal proposed work is divided into two phases' secret sharing phase and secret recovery phase.

In this paper initially proposed methodology use secret building phase, initially data packet$M^P$ can be divided into number of neighbor node and attach CRC value of rest with each phase for authentication at destination as shown in figure 2. Proposed Methodology used to calculate combine CRC for N-1 phase for any random phase. Whereas at destination end for each datagram CRC value is use to verify cheater participation. If CRC is not match then destination node send retransmission request to sender and whole process freshly repeated.

## V. SIMULATION MODEL

Simulation scenarios are constructed by varying number of nodes. In each scenario, a few nodes approximately 5-20% are included as malicious nodes. For example, if there are totally 50 nodes in the heterogeneous networks, 5 nodes of them are the malicious nodes while other nodes are correct nodes performing good communication practices.

Table 1: Simulation Parameters

| Parameters | Values | |
|---|---|---|
| Number of Nodes | Vary from 50 to 250 | |
| Area | 50 | 600*300 |
| | 100 | 600*300 |
| | 150-250 | 1000*800 |
| Traffic | CBR | |
| Simulation Duration | 100 Mili Seconds | |
| Packet Transmission Rate | 1024 kbps | |
| Carrier sense threshold Used In Normal Nodes | 200 Meter | |

## VI. PERFORMANCE EVALUATION METRICS

The performance metrics which are used to analyze the performances of routing protocols in heterogeneous ad hoc networks are discussed in the following:

- **Encryption Time overhead:** For any ideal routing protocol it is required that it has lower Encryption overhead ie share building and rebuilding time, whereas existing approach by using have required higher Encryption overhead as compare to proposed methodology as shown in figure 3

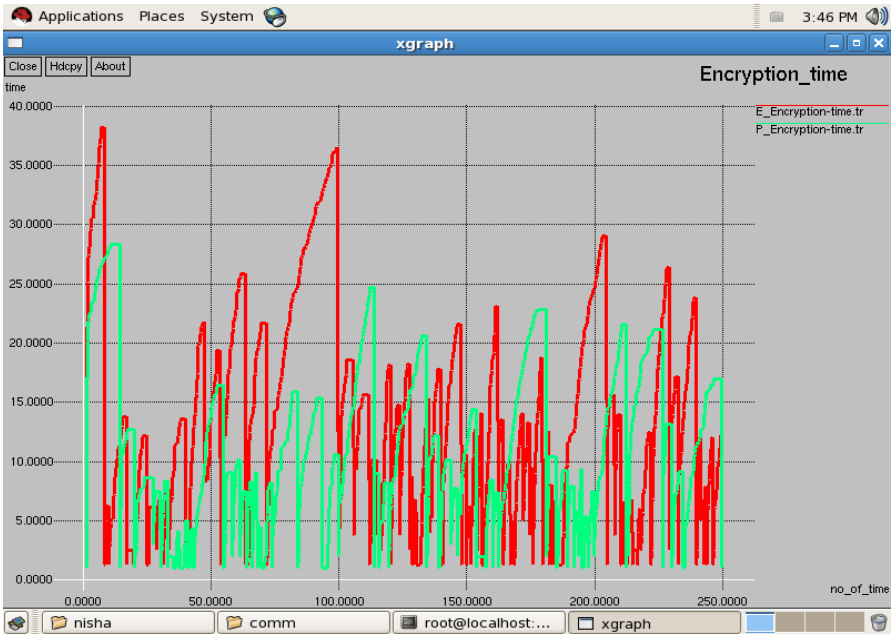


Fig.3. Encryption Time overhead

- **Recovery Ratio:** For any ideal massage share protocol it is required that it has lower recovery ratioie share lower chance to crack the authentication, whereas existing approach by using have required higher Recovery Ratio as compare to proposed methodology as shown in figure 4.

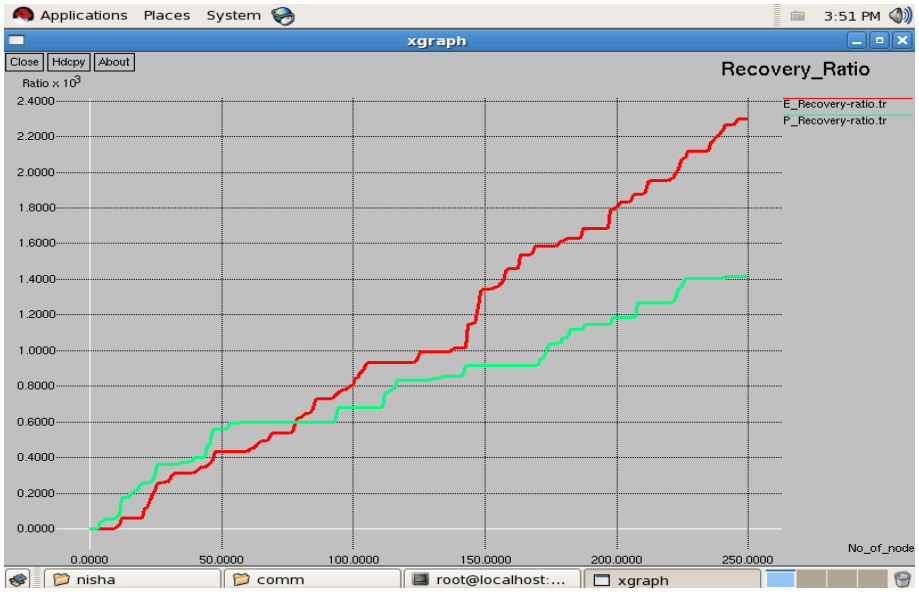

Fig.4. Recovery Ratio

- **Energy Consumption**: Energy consumption means battery power used by any node for successful transmission. Higher energy consumption degrades the survival of network. And lower energy consumption maintains longer survival of network. For any ideal conduction network need longer survival. Using this protocol the retransmission will be reduced where existing methods are only able to minimized redundant path. Existing approach have required higher battery power consumption as compare to proposed methodology as shown in figure 5.

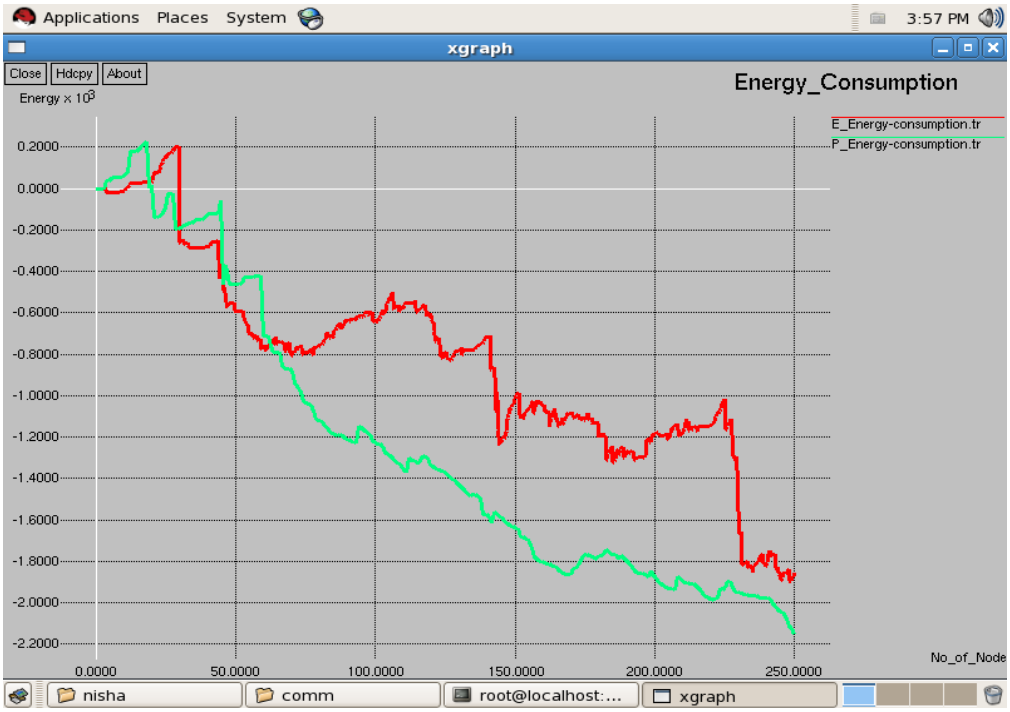

Fig.5. Energy Consumption

- **Throughput:** The fraction of the channel capacity for effective transmission (packets successfully delivered to the destination data) is given and is defined as the total number of packets received by the destination. It is in effect a measure of the efficiency of a routing protocol. In any sensor network it is required to have higher throughput ie need to increase rate of successful packet transmission as shown in figure 6.

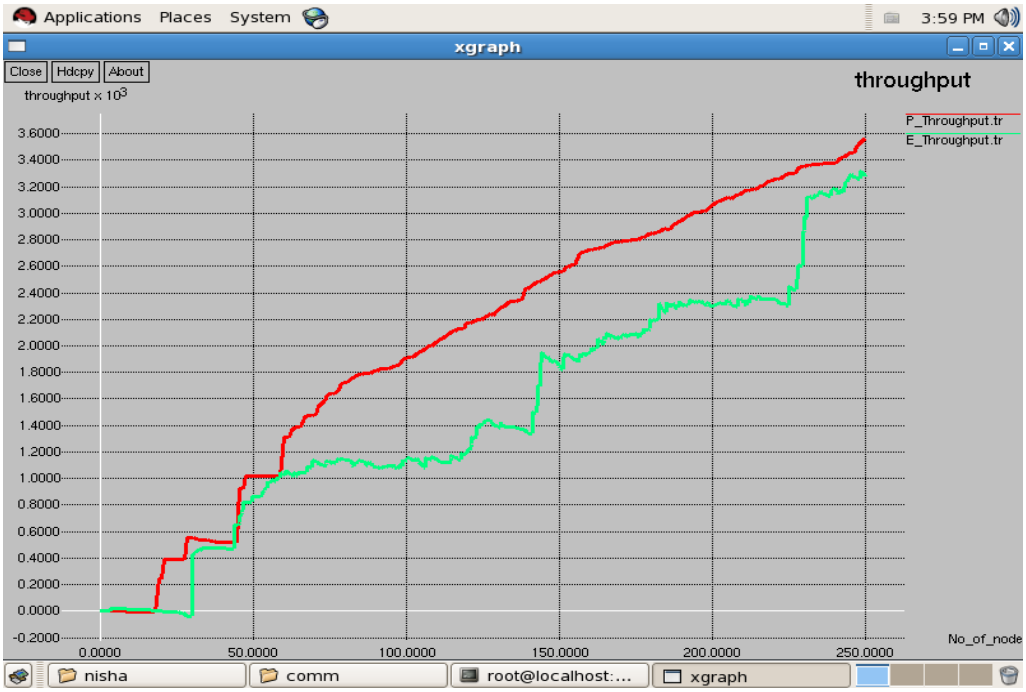

Fig.6. Throughput

## VII. Conclusion

Secret image sharing is a technique for protecting data packet that involves the dispersion of the secret datagram into many shadow datagram. This endows the method with a higher tolerance against data corruption or loss than other data-protection mechanisms, such as encryption or steganography. Because of the fast growth of wireless communication technology development.To overcome this problem this work presents an optimal approach for secret sharing. There is some problem that may occur while reconstructing the data at the reconstruction site. In this manner this dissertation has been proposing an optimal approach in order to perform secret sharing. In this paper initially proposed methodology use secret building phase, initially data packet MP can be divided into number of neighbor node and attach CRC value of rest with each phase for authentication at destination. Proposed Methodology used to calculate combine CRC for N-1 phase for any random phase. Whereas at destination end for each datagram CRC value is use to verify cheater participation. If CRC is not match then destination node send retransmission request to sender and whole process freshly repeated.

## References

[1] Toh,C.K. “Adhoc Mobile Wireless Networks:Protocols and Systems”,Prentice Hall Publications 2002.

[2] Sarkar,S.K., T.G.Basavaraju and C. Puttamadappa, “AdHoc Mobile Wireless Networks:Principles,Protocols and Applications”, AuerbachPublications, 2008.

[3] R.Billinton and R.N.Allan, “Reliability Evaluation of Engineering Systems: Conncepts and Techniques”, Springer International Edition,2nd Edition, Indian Reprint 2007.

[4] Charles J.Colbourn, “The Combinatorics of Network Reliability”,Oxford University Press, New York, 1987.

[5] Martin .L.Shooman, “Probabilistic Reliability: An Engineering Approach”, 2nd Edition Melbourne,FL,1990.

[6] M.L.Shooman, “Reliability of Computer Systems and Networks”,J.Willey,NewYork, 2002

[7] Cook JL, Ramirez-Marquez JE. “Optimal design of cluster-based ad- hoc networks using probabilistic solution discovery”,ReliabilityEngineering and System Safety 94(2009) 218-228.

[8] LaxmiShrivastava, G.S.Tomar& SS. Bhadauriya, “A Survey onCongestion Adaptive Routing Protocols for Mobile Ad-HocNetworks”, International Journal of Computer Theory andEngineering, Vol.3 No.2, pp 189-196, Apr 2011.

[9] Raghavendra CS and Hariri S., “ Reliability optimization in the design of distributed systems”, IEEE Transactions on software engineering 1985;SE-11(10):1184-93.

[10] AboEIFotoh HM, Colbourn CJ. Computing 2-terminal reliability forradio-broadcast networks. IEEE Trans Reliab 1989;38(5):538–55.163

[11] Kumar A, Pathak R, Gupta Y, " Genetic algorithm based reliability optimization for computer network expansion", IEEE transaction on reliability 1995;44(1):63-72.
[12] Dengiz B, Altiparmak F. Smith AE., "Efficient optimization of all- terminal reliable networks using an evolutionary approach", IEEE transactions on Reliability 1997;46(1):18-26
[13] Turgut D, Das SK, Chatterjee M. Longevity of routes in mobile ad hoc networks. In: Proceedings of IEEE vehicular technology conference (VTC), vol. 4, Spring; 2001. p. 2833–7.
[14] Levitin G., "Optimal allocation of multi-state retransmitters in acyclic transmission networks", Reliability Engineering and system safety 2002;75:73-82.
[15] Adickes M, Billo, R.,Norman B, Banerjee S, NnahiB,Rajagopal J,"Optimization of indoor wireless communication network layouts",IIE transaction 2002; 34:823-36.
[16] Bhatt M, Chokshi R, Desai S, Panichpapiboon S, Wisitpongphan N, et al. Impact Of mobility on the performance of ad hoc wireless networks. IEEE 58th vehicular technology conference, vol. 5, 6–9 Oct, 2003. p. 3025–9.
[17] Ye Z, Krishnamurthy SV,Tripathi SK, "A routing framework for providing robustness to node failures in mobile adhoc networks", Adhoc Networks 2004;2(1):87-107
[18] Chung W-H. Probabilistic analysis of routes on mobile ad hoc networks. IEEE CommunLett 2004;8(8).
[19] Rocco CM, Muselli M. Empirical models based on machine learning techniques for determining approximate reliability expressions. ReliabEngSystSaf 2004;83(3):301–9.
[20] Ramirez-Marquez JE, Coit DA. Heuristic for solving the redundancy allocation problem for multistate series-parallelsystems. ReliabEngSystSaf 2004; 83(3): 341–349.
[21] Marseguerra M, Zio E, Podofillini L, Coit DW. Optimal design of reliable network systems in presence of uncertainty. IEEE Trans Reliab 2005;54(2).
[22] Chen Z, Lyu MR. Reliability analysis for various communication schemes in wireless CORBA. IEEE Trans Reliab 2005;54(2): 232– 42.
[23] S. Kharbash and W.Wang, " Computing two-terminal reliability in mobile adhoc networks", proceedings of IEEE wireless communications and networking conference(WCNC '07), PP.2833- 2838, March 2007.
[24] LaxmiShrivastava, G.S. Tomar&SaritaBhadoria, "Secure and Congestion Adaptive Mechanism with Load Balancing forMANETs", International Journal of Communication Systems andNetworks, Vol.1 No.1, pp41-51, Feb 2012.
[25] Brooks, R.R, B. Pillai, S. Racunas and Suresh Rai , "Mobile Network Analysis Using Probabilistic Connectivity Matrices", IEEE transactions on System, Man and Cybernetics- Part C: Applications and Review, 2007; 37(4);694-702
[26] Cook JL, Ramirez-Marquez JE, "Two-terminal reliability analyses for mobile adhoc wireless network", Reliability Engineering and SystemSafety,2007;92(6);821-829.
[27] Cook JL, Ramirez-Marquez JE. "Mobility and Reliability Modeling for a mobile ad-hoc networks", IIE Transactions,2009;41(1);23-31.
[28] Fei Huang, Zhipeng Jiang , Sangua Zhang , SuixiangGao,Communication and Mobile Computing, DOI:10.1109/CMC.2010.49
[29] Chaturbvedi , S.K. , Padmavathy N. "The Influence of Scenario Metrics on Network Reliability of Mobile Adhoc Network"International Journal of Performability Engineering Vol 9, No. 1 , January 2013. pp .61 -74.
[30] Xibin Zhao, Zhiyang You and Hai Wan, "A Novel two-terminalreliability analysis for MANET", Journal of Applied Mathematics, volume 2013,article ID 216186
[31] LaxmiShrivastava, SS. Bhadauria, G.S. Tomar, "Influence of Traffic Load on the performance of AODV, DSR and DSDV in MANET", International Journal of Communication Systems and Network Technologies, Vol.1 Issue 1. pp 22-34, Apr 2013.
[32] Singh, M.M., Baruah, M, Mandal, J.K, "Reliability Computation of Mobile Adhoc Network Using Logistic Regression",IEEEXplore,DOI: 10.1109/WOCN.2014.6923060,2014.164
[33] K. Kobayashi, Y. Totani, K. Utsu and H. Ishii, "Improvement of Secure Communication Method Using Secret Sharing Schemes over MANET," *2015 2nd International Conference on Information Science and Security(ICISS)*,Seoul,2015,pp.1-4.doi: 10.1109/ICISSEC.2015.7371006