Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X
IMPACT FACTOR: 5.258

IJCSMC, Vol. 5, Issue. 9, September 2016, pg.179 – 185

Genetic Algorithm for Minimum Cost Blocking Problem

Dipali M. Dhaskat[1], Prof. P. L. Ramteke[2]

[1]Department of CSIT, SGBAU Amravati University, INDIA
[2]Department of CSIT, SGBAU Amravati University, INDIA
[1] dipali.dhaskat@gmail.com; [2] pl_ramteke@rediffmail.com

Abstract— Computer supported collaborative applications on overlay networks are gaining popularity among users who are geographically dispersed. Key applications is the routing protocol that directs the packet in the network routing packets fully connected to wireless networks has been studied to a great extent but the assumption on full connectivity is generally not valid in a real system. A class of attacks such as Network Partitioning Node Isolation attack spreads over the network are malicious pose majority threats which compromise the computer network evolve during their propagation and challenge to detect against the routing. We establish the provable superiority of multi-path routing protocols over conventional protocols against blocking, node-isolation and network-partitioning type attacks. We also highlight the advantages and performance issues of each routing technique.

Keywords— "Attacks, Blocking, Minimum cost blocking problem, Multipath Routing, wireless network"

I. INTRODUCTION

In wireless networks, even though the dynamic nature of networks and resource constraints entail additional overhead in maintaining and reconfiguring multiple routes, which could offset the benefits seen in wired networks, research has proven that multipath routing provides better Quality of Service guarantees. Malicious nodes can attack the network by jamming, selectively forwarding packets, black-hole attack and spoofing. In the case of statically deployed, dense Wireless Networks which use flat routing, alternate path for secure transmission on packets across such malicious nodes have to be found. We establish the provable superiority of multi-path routing protocols over conventional protocols against blocking, node-isolation and network-partitioning type attacks. These results are verified through simulations which demonstrate the robustness of multi-path routing protocols against such attacks. To the best of our knowledge, this is the first work that theoretically evaluates the attack-resiliency and performance of multi-path protocols with network node mobility. In the routing protocol design of mobile nodes, many issues need to be considered in order to offer many important properties such as scalability, security, low power consumption and so on.

Wireless Networks are considered as the underlying representative network model. They have a unique system architecture where they have nodes communicating wirelessly over multiple hops to a backbone network though multiple available network gateways. Primary traffic in the wireless network is between the backbone network and mobile nodes/stationary. These make wireless network ideal candidates for applying the full scope of any wireless multi-path protocols and study the impact of these attack scenarios.

A. *Impact and Relevance*

This theory is represented the dependability of interconnection networks, their performance, and fault tolerance under various attack scenarios. The research reported here is largely theoretical and establishes the superiority of multipath routing protocols in the face of malicious attacks. The impact and relevance pertain to building confidence on existing schemes which primarily rely on the robustness of multi-path protocols. The impacted areas would include load balancing, network coding and threshold cryptography, in the wireless domain.

- Active attack scenarios for recovery and resiliency. This work is highly relevant for scenarios where it may be easier (or harder) for the adversary to compromise some nodes in the network, as compared to compromising the rest of the nodes. For example, it would usually be more difficult (in terms of cost) to block nodes closer to the gateways or Base Stations (BS) due to reasons of physical proximity (physically better guarded), or signal strength (nodes closer to BS may have better received signal strength). Similarly, it is highly desirable for protocols to continue to execute correctly without information compromise, even in the presence of a few malicious nodes. Currently, most security protocols do not address recovery from malicious behavior. Protocols simply abort execution and restart if any malicious behavior is detected. This is detrimental especially in applications where real-time response and high level security are important as information may have already been lost in the partial execution and frequent restart of the protocols.
- Relevance and impact on existing protocols. Multi-path routing protocols can naturally extend threshold cryptography concepts to the wireless domain. Demonstrated robustness of multi-path protocols against such blocking type attacks would increase confidence in utilizing threshold cryptography schemes. In threshold cryptography, a node splits a secret into several shares, routes them along independent paths, and a threshold number of shares have to be compromised (at least) for an adversary to recover the secret. Our results imply that it would be at least exponentially hard for an adversary to optimally compromise or block certain threshold number of shares such that either the adversary recovers the secret, or equivalently, the secret is not recovered properly at the destination. Network coding, where nodes intelligently send redundant information along multiple paths to ensure security and reliability and to detect any problems with a route would also benefit from such demonstrated robustness of multi-path routing. Again, it would be at least exponentially hard for the adversary to optimally compromise more than a threshold number of these paths to render such network coding schemes ineffective.

B. *Contributions*

While there has been some work on integrating the benefits provided by multi-path routing protocols with security mechanisms, there exists a gap in analyzing multi-path routing attacks. Specifically two areas that need to be analyzed are:

- The performance in terms of security and resiliency of mobile wireless networks multi-path protocols under different attack scenarios, and
- Comparison with traditional single-path protocols under such circumstances. The identification of the Minimum Cost Blocking (MCB) problem.

Though we consider MCB in the WMN setting, the problem is applicable to other wireless or wired networks. Evaluating the hardness of the problem. MCB is NPhard for the low/no node mobility scenario and #P-hard for networks with patterned node mobility. Development of genetic algorithms for the best case scenario and the performance testing of these algorithms in different settings through random graphs based experiments. Laying direction for future research to evaluate the performance of multi-path protocols against sophisticated attacks in mobile wireless networks.

C. *Motivation*

Multi-path routing protocols unlike standard routing protocols intend to discover multiple paths between a source and a destination node. Their utility lies in compensating for the dynamic and unpredictable nature of networks. Specifically, the multiple paths provide load balancing, fault tolerance and higher aggregate bandwidth. It has been proven that using multi-path routing in dense networks enhances performance and result in better throughput than unipath routing. Traditionally, multi-path routing has been in the context of WMNs. But recently, there has been progress in adapting these protocols to other types of networks such as Wireless Network. The two main components of multi-path routing are discovering routes and then maintaining these routes based on certain metrics. Examples of such metrics include Estimated Transmission Count (ETX) , Expected Transmission Time (ETT), etc. present a new multipath routing protocol for heterogeneous networks where they choose QoS as a routing metric. However, it is important to note that unlike unipath routing, multi-path routing metrics are aggregate in nature, i.e., paths at each hop are chosen to maximize/minimize the sum of the individual paths at each hop and not choose the best path each hop.

To reiterate, since multi-path routing protocols are intended to increase (decrease) say aggregate bandwidth (end to end delay, for instance), the routes selected by these protocols need to facilitate it. This implies that such routes need to be disjoint (not have any common nodes or links) to increase fault tolerance, since the failure of a single node/link can cripple the entire network and be detrimental to the multipath routing philosophy. However, the cost for discovering such routes is expensive in terms of both time and resources. Further, because of the nature of networks, non-disjoint routes are more abundant. Additionally, node-disjointness (no common node between two paths) is a stricter requirement than even link-disjointness (no common link between two paths), making them least abundant and thus, hardest to find. Due to these practical considerations, in most multi-path routing, more often than not non-disjoint routes are selected. This causes a huge security risk, since the compromise of such paths could effectively partition the network. While such a problem does arise with even unipath routing because of the aggregate nature of metrics in multi-path routing, it is more severe in multi-path routing.

multi-path routing in wireless networks. When we use unipath for sending packets from source to destination. Path will block sometimes so that packet does not reach to destination. If we used unipath, it also takes time for sending packet. So we used multipath routing protocol for minimum cost blocking problem. From the works surveyed, AODV-DM emerged as a protocol able to find non interfering routes with a reasonable signaling cost. Unfortunately, the latency in the discovery of the second route seemed very large. Our first idea was to modify the protocol in an attempt to speed up the route discovery process. Eventually, this effort leads to the design of a cluster-based algorithm for route discovery and maintenance. Multi-path traffic scheduling and routing protocols in wired networks are deemed superior over conventional single path protocols in terms of both enhanced throughput and robustness. In wireless networks, even though the dynamic nature of networks and resource constraints entail additional overhead in maintaining and reconfiguring multiple routes, which could offset the benefits seen in wired networks, research has proven that multi-path routing provides better Quality of Service guarantees. Blocking, node-isolation and network-partitioning type attacks are easy to launch and are effective in the wireless networks domain due to channel constraints and dynamic network topologies.

II. EXISTING SYSTEM

The initial goal of this work was to study and analyze techniques to support multi-path routing in wireless mesh networks. From the works surveyed, AODV-DM emerged as a protocol able to find non interfering routes with a reasonable signaling cost. Unfortunately, the latency in the discovery of the second route seemed very large. Our first idea was to modify the protocol in an attempt to speed up the route discovery process. Eventually, this effort leads to the design of a cluster-based algorithm for route discovery and maintenance.

MULTI-PATH traffic scheduling and routing protocols in wired networks are deemed superior over conventional single path protocols in terms of both enhanced throughput and robustness. In wireless networks, even though the dynamic nature of networks and resource constraints entail additional overhead in maintaining and reconfiguring multiple routes, which could offset the benefits seen in wired networks, research has proven that multi-path routing provides better Quality of Service (QoS) guarantees.

III. RELATED WORK

Multipath routing is to allow the use of several good paths to reach destinations achieved without imposing excessive control overhead in maintaining multiple paths between a source and a destination. Redundancy in the network or providing backup routes to be used when there is a failure are forms of introducing fault tolerance at the routing level in wireless networks which consists in modifying the route of a packet if the actual route broken. Bandwidth routing along single path may not provide enough bandwidth for a connection using simultaneously multiple paths to route data can be good approach to satisfy the bandwidth requirement of some applications. Suppose traffic distribution is not equal in all links in the network spreading the traffic along multiple resources can alleviate congestion in some links. Multipath protocols can be used to provide error resilience by distributing traffic over multiple paths, security routing protocols is easy for an adversary to launch routing attacks but multipath offers attack resilience. For comparison purposes, we also launch similar attacks on conventional single-path protocols and measure their impact. As we consider multipath routing protocols, the attacker has to consider the operation of multi-path routing since multiple paths will exist from the source to the destination. This attack cost due to the nodes close proximity to base stations. In a black hole attack, a particular node in a network falsely advertises a route based on metrics specific to the protocol to the destination node so as to force the route discovery algorithm to choose a route through in it.

However, it has to be also noted that multi-path routing is not necessarily affected by wormhole attacks. We do not consider black hole and wormhole attacks explicitly in this paper. Further, Sybil attack where a node can be assigned multiple identities is precluded from our threat model since the focus is on primarily the blocking attack. In a genetic algorithm, many individual solutions are randomly generated to form an initial population. This population then evolves over successive generations to give better solutions. Each generation is comprised of various phases, the most important being fitness evaluation, selection, reproduction and mutation.

IV. MULTIPATH ROUTING

Multipath routing was used to enhance the reliability of wireless network. The proposed scheme is useful for delivering data in unreliable environments. It is known that network reliability can be increased by providing several paths from source to destination and sending the same packet on each path. However, using this technique, traffic will increase significantly. Hence, there is a trade-off between the amount of traffic and the reliability of the network. This tradeoff is studied in using a redundancy function that is dependent on the multipath degree and failing probabilities of the available paths. The idea is to split the original data packet into sub packets and then send each sub packet through one of the available multipath. It has been found that even if some of these sub packets are lost, the original message can still be reconstructed. According to their algorithm, it has also been found that for a given maximum node failure probability, using a higher multipath degree than a certain optimal value will increase the total probability of failure. Directed diffusion is a good candidate for robust multipath routing and delivery. Based on the directed diffusion paradigm, a multipath routing scheme that finds several partially disjoint paths is studied in alternate routes are not node disjoint, i.e., routes are partially overlapped.

It has been found that the use of multipath routing provides a viable alternative for energy-efficient recovery from failures in wireless network. The motivation for using these braided paths is to keep the cost of maintaining the multipath low. The costs of alternate paths are comparable to the primary path because they tend to be much closer to the primary path. Some sophisticated routing protocols support multiple paths to the same destination. Unlike single-path algorithms, these multipath algorithms permit traffic multiplexing over multiple lines. The advantages of multipath algorithms are obvious: They can provide substantially better throughput and reliability. This is generally called load sharing

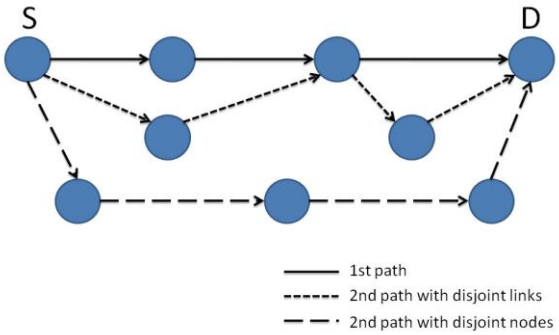

Fig. 1 Multipath Routing

A. *Proactive routings*

With table-driven routing protocols, each node attempts to maintain consistent, up-to-date routing information to every other node in the network. This is done in response to changes in the network by having each node update its routing table and propagate the updates to its neighboring nodes. Thus, it is proactive in the sense that when a packet needs to be forwarded the route is already known and can be immediately used. As is the case for wired networks, the routing table is constructed using either link-state or distance vector algorithms containing a list of all the destinations, the next hop, and the number of hops to each destination. Many routing protocols including Destination-Sequenced Distance Vector (DSDV) and Fisheye State Routing (FSR) protocol belong to this category, and they differ in the number of routing tables manipulated and the methods used to exchange and maintain routing tables.

B. *Reactive routing*

With on-demand driven routing, routes are discovered only when a source node desires them. Route discovery and route maintenance are two main procedures: The route discovery process involves sending route-request packets from a source to its neighbor nodes, which then forward the request to their neighbors, and so on. Once the route-request reaches the destination node, it responds by unicasting a route-reply packet back to the source node via the neighbor from which it first received the route-request. When the route-request reaches an intermediate node that has a sufficiently up-to-date route, it stops forwarding and sends a route-reply message back to the source. Once the route is established, some form of route maintenance process maintains it in each node's internal data structure called a route-cache until the destination becomes inaccessible along the route Note that each node learns the routing paths as time passes not only as a source or an intermediate node but also as an overhearing neighbor node. In contrast to table-driven routing protocols, not all up-to-date routes are maintained at every node. Dynamic Source Routing (DSR) and Ad-Hoc On-Demand Distance Vector (AODV) are examples of on-demand driven protocols.

V. MCB IN WIRELESS NETWORKS

A class of Minimum Cost Blocking (MCB) problems in Wireless Networks with multi-path routing protocols is presented in paper. We establish the provable superiority of multi-path routing protocols over conventional protocols against blocking, node-isolation and network-partitioning type attacks. In our attack model, an adversary is considered successful if he is able to capture/isolate a subset of nodes such that no more than a certain amount of traffic from source nodes reaches the gateways. The general problem of blocking possible traffic flow between a pair of the vertices in a connected graph is known as the max-flow min-cut problem. In this section, we first consider to a particular case of blocking between a pair of nodes in wireless networks. The adversary can now stage an attack by blocking some nodes in the network such that all traffic between a certain pair of nodes will pass through at least one of the compromised nodes. Though this is conceivable, we show that it is NP hard to find the minimum cost set of nodes so that all traffic between the source destination pair will pass through the one of the compromised nodes.

We now present the Multi-path MCB problem for the stationary-nodes/low-mobility scenario. The network is modelled as an undirected graph G, with vertex set V and edge set E. Here, every vertex represents a node in the network and a link between two vertices implies that corresponding nodes are within each other's radio range. A directed graph may better represent the network for real-world situations since nodes may have different radio ranges, signal strength may be different in each direction, and links may not be completely bidirectional. However for simplifying the problem description we assume an undirected graph, emphasizing that all our results are equally applicable to the general case of directed graphs.

VI. MCB PROBLEM

Most of the routing protocols that have been proposed for mesh and ad hoc networks are unipath, which means only a single route is used between a source and a destination node. The main goal of multipath routing is to allow the use of several good paths to reach destinations, not just the best path. This should be achieved without imposing excessive control over head in maintaining such paths. The availability of multiple paths between a source and a destination can be used to achieve the following benefits:

- Fault tolerance: introducing redundancy in the network or providing backup routes to be used when there is a failure, are forms of introducing fault tolerance at the routing level in wireless networks.
- Throughput enhancement: in a mesh network, some links can have limited bandwidth. Routing along a single path may not provide enough bandwidth for a connection.
- Error resilience: multipath protocols can be used to provide error resilience by distributing track (for instance, using data and error correction codes) over multiple paths.
- Security: with single-path routing protocols, it is easy for an adversary to launch routing attacks, but multipath offers attack resilience.

We now present the Multi-path MCB problem for The stationary-nodes/low-mobility scenario. The network is modelled as an undirected graph *G*, with vertex set *V* and edge set *E*. Here, every vertex represents a node in the network and a link between two vertices implies that corresponding nodes are within each other's radio range. A directed graph may better represent the network for real-world situations since nodes may have different radio ranges, signal strength may be different in each direction, and links may not be completely bidirectional. However for simplifying the problem description we assume an undirected graph, emphasizing that all our results are equally applicable to the general case of directed graphs.

VII. GENETIC ALGORITHM

A Genetic Algorithm is a metaheuristic technique that is used to solve different optimization problems by imitating natural selection; i.e., the operation of adaptation to the environment carried out by living beings. GAs are an attractive method to solving the complex problem summarized in the previous section. A GA determines a whole 'population' of 'individuals', which are candidate solutions to the optimization problem. The distinguishing characterizes of each individual are coded into a structure called a 'chromosome'. The chromosome is a structure of genes, whose values can be selected from within a set of symbols. An application-dependant operation creates the individual by decoding its chromosome. The symbols employed as values of the genes are typically integer, real, or binary numbers, rely on the type of the problem. Once an individual is created, a fitness function is used to evaluate its fitness as a solution to the problem. Low values of fitness function are typically determined to the most fit individuals (minimization problem).

A GA begins with an initial population created either randomly or with some heuristic method that exploits the information of an expert in the problem area. The algorithm then advances in steps called generations. At each generation *g*, a new population $P(g + 1)$ is developed from $P(g)$. As generations pass, the population should globally improve on account of the application of genetic operators that imitate natural evolutionary techniques. To this end, the most fit individuals are chosen from $P(g)$ (selection) to be mated (crossover) and partially adjusted (mutation) so as to generate the new population $P(g + 1)$. The selection operation is used to determine which individuals in $P(g)$ should be selected to generate $P(g + 1)$ Optionally, an elite from among the

chosen individuals (i.e., a small number of the best proceeding individuals) survives and is passed from $P(g)$ to $P(g + 1)$ without change. The crossover operation consists in choosing some of the individuals and mating them. In other words, it substitutes them with their children; i.e., individuals produced by mixing the genetic item in the parents' chromosomes. The real working of a crossover operation greatly depends on the encoding of the chromosome. Finally, the mutation operation presents some new genetic item in the population by randomly modifying the values of some genes. Many kinds of mutation operations can be identified to treat with different sets of symbols. The population continues to improve until a stopping criterion is achieved, with the simplest being a maximum number of generations. In addition, GA can be regarded as rapid steps for determining a 'good enough' solution to the problem; therefore they are interesting for practical problems [32]. GA is directly applicable, which allows them benefit with respect to the exact techniques. Therefore, a GA can be used to work in WMN design in which the solution may be iteratively updated.

A chromosome of the proposed GA consists of sequences of positive integers that represent the IDs of nodes through which a routing path passes. Each locus of the chromosome represents an order of a node (indicated by the gene of the locus) in a routing path. The gene of first locus is always reserved for the source node. The length of the chromosome is variable, but it should not exceed the maximum length , where is the total number of nodes in the network, since it never needs more than number of nodes to form a routing path. A chromosome (routing path) encodes the problem by listing up node IDs from its source node to its destination node based on topological information database (routing table) of the network. The information can be easily obtained and managed in real-time by routing protocols such as RIP, OSFP, DSDV, DSR and VCRP in wired or wireless environments, but the detailed mechanisms or other controversial issues are beyond the scope of this paper. It is noted that the topological information database of the network can be constructed easily and rapidly by such routing protocols.

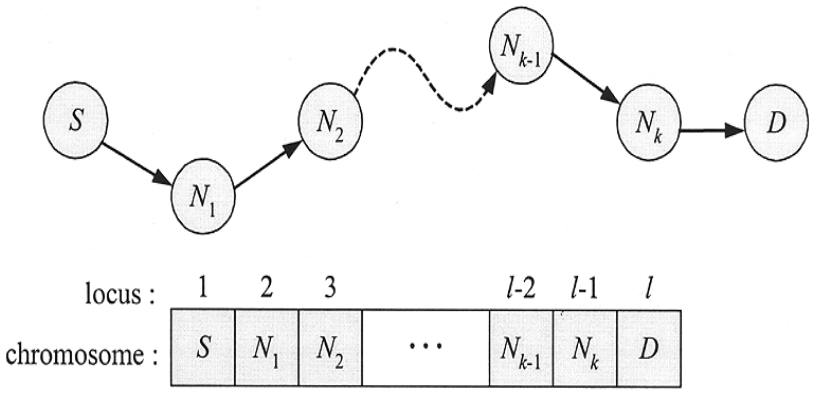

Fig. 2 Example of routing path

An example of chromosome (routing path) encoding from node to node is shown in Fig. The chromosome is essentially a list of nodes along the constructed path, In Fig represents the total number of nodes forming a path The gene of the first locus encodes the source node, and the gene of second locus is randomly or heuristically selected from the nodes connected with the source node that is represented by the front gene's allele. A chosen node is removed from the topological information database to prevent the node from being selected twice, thereby avoiding loops in the path. This process continues until the destination node is reached. It is noted that an encoding is possible only if each step of a path passes through a physical link in the network.

A. *Population Initialization*

In general, there are two issues to be considered for population initialization of GAs: the initial population size and the procedure to initialize the population. It was felt that the population size needed to increase exponentially with the complexity of the problem (i.e., the length of the chromosome) in order to generate good solutions. Recent studies have shown, however, that satisfactory results can be obtained with a much smaller population size. To summarize, a large population is quite useful, but it demands excessive costs in terms of both memory and time. As would be expected, deciding adequate population size is crucial for efficiency. Secondly, there are two ways to generate the initial population: heuristic initialization and random initialization. Although the mean fitness of the heuristic initialization is already high so that it may help the GAs to find solutions faster, it may just explore a small part of the solution space and never find global optimal solutions because of the lack of diversity in the population. Therefore, random initialization is effected so that the initial population is generated with the encoding method already explained in Section II-A. Physically, the random initialization chooses genes (nodes) from the topological information database in a random manner during the encoding process. It is possible that the algorithm encounters a node for which all of whose neighboring nodes have already been visited. In this case, the defective chromosome is refreshed and

reinitialized. This may induce a subtle bias in which some partial paths are more likely to be generated. However, the meager bias does not significantly affect the performance of the algorithm.

B. *Fitness factor*

The situation where the intention is to find a solution. This focuses on devising the fitness function itself and testing with different values of the fitness function. Determining the appropriate fitness function With combinatorial optimization problems (more than one parameter) and where there are many constraints, most points in the search space often represent invalid chromosomes, hence having a zero "true" value. For a GA to operate successfully, a fitness function needs to be created where the fitness of an individual chromosome is seen in terms of how it is leading us towards valid chromosomes. This is in fact a sort of catch-22 situation, it should be known where the valid chromosomes are to ensure that the nearby points can also be given a good fitness values, and far away points given poor fitness values, but if it is not known where the valid chromosomes are this cannot be achieved. It has been suggested by Cramer (8) that if the goal of the problem is all or nothing, better results can be obtained if meaningful sub-goals are invented. These sub-goals should then be rewarded.

VIII. CONCLUSIONS

In this paper we have describe the Minimum cost blocking Problem in multipath wireless routing protocol. Our paper presents blocking of attacks in wireless network in secure manner which evaluate the normal or abnormal activities and also the comparison of proposed solution. We believe that the results of our research will impact a number of areas including the security and robustness of routing protocols in mesh networks, threshold cryptography and network coding. Moreover, even though we do not necessarily consider insider attacks, we would like to point out that our analysis does allow for an attacker to possess topological information of the network, which is the case of an insider attack.

ACKNOWLEDGEMENT

Thank to Prof. P. L. Ramteke, HOD, Department of computer science and information technology, HVPM COET, Amravati, India.

REFERENCES

[1] Danyan Luo, Decheng Zuo, Xiaozong Yang "An Energy-Saving Routing Protocol for Wireless Sensor Networks" IEEE Wireless Communications, April 2008

[2] L. Ting-Yu, H. Kai-Chiuan, H. Hsin-Chun, Applying genetic algorithms for multiradio wireless mesh network planning, IEEE Transactions on Vehicular Technology, vol. 61, no. 5, pp. 2256–2270, June 2012.

[3] S. Sakamoto, E. Kulla, T. Oda, M. Ikeda, L. Barolli and F. Xhafa, "A comparison study of simulated annealing and genetic algorithm for node placement problem in wireless mesh networks", Journal of Mobile Multimedia, vol. 9, pp.101-110, 2013

[4] Christoph Sommer and Falko Dressler "The DYMO Routing Protocol in VANET Scenarios" Journal of Computer Networks and Communication Systems,vol .8 ,may 2011

[5] D. Ganesan, R. Govindan, S. Shenker, and D. Estrin, "Highly- Resilient, Energy-Efficient Multipath Routing in Wireless Sensor Networks," SIGMOBILE Mobile Computer Comm. Rev., vol. 5, pp. 11-25, Oct. 2001.

[6] S. Chen and M. Wu, "Anonymous Multipath Routing Protocol Based on Secret Sharing in Mobile Ad Hoc Networks," J. Systems Eng. and Electronics, vol. 22, no. 3, pp. 519-527, June 2011.

[7] Qi Duan, Mohit Virendra, Shambhu Upadhyaya "Minimum Cost Blocking Problem in Multi-Path Wireless Routing Protocols," IEEE TRANSACTIONS ON COMPUTERS, vol. 63, no. 7, July 2014.

[8] Molly Mehra, M.L. Jayalal, R. Jehadeesan, S. Rajeswari, S.A.V. SatyaMurty "Genetic Algorithm Based Risk-Cost Analysis of Neutron Flux Monitoring System for Prototype Fast Breeder Reactor" IEEE ICRTIT 2011 MIT, Anna University, Chennai. June 5, 2011.

[9] C.-K. Chau, R. Gibbens, R. Hancock, and D. Towsley, "Robust Multipath Routing in Large Wireless Networks," Proc. IEEE INFOCOM '11, pp. 271-275, Apr. 2011.

[10] Y. Kato and F. Ono, "Node Centrality on Disjoint Multipath Routing," Proc. IEEE 73rd Vehicular Technology Conf., May 2011.

[11] Jamal N. Al-karaki, Ahmed E. Kamal "ROUTING TECHNIQUES IN WIRELESS SENSOR NETWORKS" IEEE Wireless Communications, December 2004.

[12] M. Razzaque and C. Hong, "Analysis of Energy-Tax for Multipath Routing in Wireless Sensor Networks," Annals of Telecomm, July 2010.

[13] R. Ahlswede, N. Cai, S.-Y. R. Li, and R. W. Yeung, "Network information flow" *IEEE Trans. on Information Theory*, 2000.

[14] S.-Y. R. Li, R. W. Yeung, and N. Cai, " Linear network coding, " *IEEE Transactions on Information Theory*, 2003

