International Journal of Advanced Computer Technology (IJACT)

ISSN:2319-7900

A Genetic Approach for Optimized Routing in Wireless Mesh Networks

R. Kalpana, Department of Computer Science & Engineering, Pondicherry Engineering College;
Kumar Navneet, Department of Computer Science & Engineering, Pondicherry Engineering College

Abstract

In a Wireless Mesh Network (WMN), high speed routers equipped with advanced antennas, communicate with each other in a multi-hop fashion over wireless channels and form a broadband backhaul. WMNs provide fault-tolerance and reliable connectivity, as each node is connected to several other nodes. The neighbors of a node can find another route, if a node fails due to hardware problems. Extra capacity can be achieved by introducing additional nodes in the network. However, the throughput of a WMN may be severely degraded due to presence of some selfish routers that avoid forwarding packets for other nodes even as they send their own traffic through the network and this introduces unnecessary delay in delivery of valid packets. This paper presents a genetic approach for detection of selfish nodes as well as optimization of routing time in a WMN.

.

1. Introduction

Wireless mesh network (WMN) as name suggests is a communication network having mesh topology consisting of radio nodes. WMN's consist of mesh clients, mesh routers and gateways. Laptops, cell phones and other wireless devices are called as mesh clients, the mesh routers forward traffic to and from the gateways which may but need not connect to the Internet. Mesh cloud is the coverage area of the radio nodes working as a single network. The working in harmony of radio nodes with each other to create a radio network decides the access to mesh cloud. A mesh network is reliable and offers redundancy. When one node can no longer operate, the rest of the nodes can still communicate with each other, directly or through one or more intermediate nodes. A special type of wireless ad-hoc network is a wireless network. The difference between a wireless mesh network and an ad-hoc network is that a wireless mesh network often has a more planned configuration, and may be deployed to providedynamic and cost effective connectivity over a certain geographic area whereas an ad-hoc network, is formed when wireless devices come within communication range of each other. The mesh routers can be mobile, and be moved according to specific demands arising in the network. The mesh routers are mostly not limited in terms of resources compared to other nodes in the network and hence can be exploited to perform more resource intensive functions.

In this way, the wireless mesh network differs from an ad-hoc network, because these nodes are often constrained by resources. Nodes comprise of mesh routers and mesh clients. Each node operates both as a host and also as a router, forwarding packets on behalf of other nodes that may not be within direct wireless transmission range of their destinations. A WMN is dynamically self-organized and self-configured, with the nodes in the network automatically establishing and maintaining mesh connectivity among themselves.

1.1 Routing Attacks in WMNs

In this section, we consider the attacks that affect the network layer as well as the MAC layer of WMN. These attacks exploit the channel assignment androuting algorithms in multi-radio multi-channel wireless mesh networks (MR-MC WMN).The major limitation for wireless mesh networks is Bandwidth capacity. To increase the available bandwidth in MR-MC WMN, each WMN node is equipped with multiple radios (NICs). At each interface of the node orthogonal channels are used for simultaneous communication using all the wireless interfaces without interference. Dynamic channel assignment is required to assign the channels to the network links. The objective of the channel assignment algorithms is to ensure the minimum interference within WMN. Various channel assignment andjoint routingalgorithmshave been proposed for (MR-MC WMN) [1, 2, 3, 4, 5].
Note that routing is done at the network layer functionality while the channel assignment is done at the MAC layer. All the channel assignment andjoint routing algorithms assume that the mesh nodes are well-behaved. Hence the nodes make independent decision about their channel assignment based on the neighbors channel assignment information and inform neighboring nodes about the decision which is not verified. The independent decision of the nodes and the assumed trust amongst the WMN nodes make these algorithms vulnerable to security attacks.

Network endo-parasite attack (NEPA)[6,7]is launched by the compromised malicious node when it changes the channel assignment of its interfaces in such a way that the interference on heavily loaded high priority channels increases (Each interface is switched to a different high priority channel). This is contrary to the normal operation of the channel assignment algorithm where the node assigns the least loaded channels to its interfaces.

Channel ecto-parasite attack (CEPA)[6,7] is a special type of NEPA. During CEPA, the malicious node switches all its interfaces to the most heavily loaded highest priority channel. Like NEPA, the malicious node does not inform its interference domain neighbours about the change in channel assignment. The effect of the attack is the hidden usage of the most heavily loaded channel which increases the interference considerably resulting in a decrease in performance.

Low cost ripple effect attack[6,7] is launched when the compromised malicious node transmits misleading channel assignment information about its interfaces to the neighboring nodes without actually changing the channel assignment. The information is calculated in such a way that the neighboring nodes are forced to adjust their channel assignments in order to minimize the interference which may generate a series of changes even in the channel assignment of the nodes that are not direct neighbors of the malicious node.

1.2 Characteristics of Security Solution for Wireless Mesh Networks

In the previous section, the security attacks that exploit the vulnerabilities in the network layer protocols for WMN and MAC layer is discussed. In order to successfully prevent, detect and counteract these attacks, essential characteristics that a security mechanism for WMN are listed below

- In wired networks, on per link basis the security services of data integrity and data confidentiality are generally provided (between two devices), by assuming that end devices are secure. However, the WMN nodes may resort to the selfish and malicious behavior. In order to prevent the selfish and malicious behavior of the intermediate hop nodes, the WMN must provide the end-to-end services of data integrity and data confidentiality, in addition to the security services on per link basis.
- The trust establishment mechanism should be robust against malicious behavior and internal selfish. Note that the malicious behavior and internal selfish are part of WMN therefore the conventional authentication mechanisms based on cryptographic primitives may not be effective against the internal misbehavior.
- Wireless mesh networks are self-administered networks and lack the centralized administration authority which can respond to the network issues. Therefore, the attack and anomaly detection mechanisms for wireless mesh networks must not be dependent on the administrator and should be self – sufficient to verify the possible attack and anomaly alerts.
- Self-healing nature is an important characteristic of wireless mesh networks. Therefore, the detection mechanisms must be coupled with adequate automated response to the security attacks and identified anomalies.

2. Related Work

Numerous intrusion detection techniques have been proposed at the network layer for wired as well as wireless networks. Some of the recent research efforts related to this domain is discussed here. Most of the intrusion detection systems rely on the data mining techniques and knowledge based systems [8, 9, 10]. For example HuangET. al. [6] have proposed IDS based on the cross-feature analysis for multi-hop mobile wireless networks. Different parameters in the network are monitored by the node and based on values of i-1 parameters, predict the value of i_{th} parameter and compare it with monitored value of that parameter to detect routing anomalies in the networks. As an extension to this work authors have also proposed the distributed cluster based approach [10] where they propose the division of network into clusters and only few elected nodes within each cluster perform the monitoring with the intrusion detection probability almost same as with all the nodes actively monitoring. The primary design goal for wireless networks is resource efficient, this scheme satisfies the design goal.

For mobile ad hoc networks Yang et. al. [7] has proposed the self-organized network layer security solution. This is one of the very few solutions which ensure self-organized and self-healing network. The solution is based on information cross-validation and distributed neighbour collaboration, resulting in self-healing/self-organized network. The scheme is based on the threshold secret sharing. Novel token based crediting scheme have been proposed by authors. After some time duration the token of the node expires. The token expiry time of the node based upon the credit of the node. Over the period of time the credit of the well behaving nodes gets accumulated. Therefore, the token expiry time of these nodes is longer and is linearly incremented every time the node refreshes its token. The token of malicious or selfish nodes is revoked by neighbour collaboration refraining them to participate in the network. Using routing protocols well behaving and malicious nodes are differentiated and consist of packet forwarding ratio,hop count distance etc. The intrusion detection mechanisms at the network layer primarily address the issues of selfish, malicious and misbehaving nodes that are at the heart of almost all the attacks at network layer. The solutions like

[9,10] identify the anomalies in the control messages to detect the control plane attacks like wormhole attack, rushing attack, grey hole attack, black hole attack, routing loop attack and network partitioning attack. On the other hand, the data plane attacks are detected using neighbour monitoring techniques [7].

Ant Colony Optimization (ACO) based routing [11] is applied Wireless Mesh networks. Fuzzy logic based hybrid integrated link cost metric that took into account throughput, delay, and jitter of the link and residual energy of the node as performance parameters.

3. Optimization Using Genetic Algorithm

It is clear that AODV depends heavily on cooperation among the nodes for its successful operation. A selfish node can easily manipulate the protocol to minimize its chances of being included on a route for which it is neither the source nor the destination. Alternatively, it may drop, delay, or modify the RREP messages so as to prevent the replies from reaching the source node. The algorithm attempts to detect such selfish behavior of nodes in a WMN.

3.1 Genetic Algorithms

The GA, which was introduced by John Holland, was adopted from natural evolution. The following are the features of Natural evolution:

1)Encoding of characteristics of an individual on a chromosome.

2) Each chromosome has certain fitness according to the environment in which it exists.

3)According to environment it exists, each chromosome has certain fitness.

4)Individuals who are estimated to be stronger can be able to survive and can produce future generation of stronger individuals.

- The GA is established on the features mentioned above in the following manner: the result of the problem is encoded on a string which is comparable with the chromosome of the biological system.
- The GA maintains a population of arbitrarily selected chromosomes and permits filter chromosomes to aggregate and give rise offspring with new characteristics, which may substitute low fitness old chromosomes. This is repeated until we find a chromosome with best characteristics, which symbolizes the optimal solution of the problem.

There are two mechanisms that link a genetic algorithm to the problem it is solving. These two mechanisms are:

1) Encoding solutions to the problem on chromosomes.

2) Evaluation function that returns a measurement of the worth of a chromosome in the context of the problem.

This is what is called as the fitness of a chromosome. The evaluation function plays the same role in the genetic algorithm that the environment plays in natural evolution.

In order to use GA's for network topological design, the chromosome is chosen to contain the network parameters. A possible chromosome would be a string containing the weights of all nodes of the network. The evaluation function which assigns fitness to each chromosome is chosen according to the objective of the design problem. If the objective is to minimize the route between source and destination, then the evaluation function will compute the all distances of all possible paths between source and destination and give the dynamic optimal path with time change.

3.2 Routing Optimization Using Genetic Algorithm

- To enhance the routes stability and to discover the optimal paths from the available multiple paths, genetic algorithm is carried out in inherent protocol. Firstly by using the concepts of AODV multipath routing protocol, multiple paths available can be found from source to destination node.
- Having a set of routes at hand, the source disseminates each outgoing message into a number of pieces and each piece routed through a different path.
- The destination corroborates the incoming pieces and acknowledges the successfully received ones through a feedback back to the source. In this manner, the source receives authentic feedback that explicitly determines the piece that was received by the destination. A piece that was received successfully means that the corresponding route is functional, while a failure is a firmly show that the route is either broken or compromised.
- A path is discarded once it is viewed as failed and a precaution should be taken not to use the same path, if it is found again within erst while after it has been discarded.

4. Simulation

In this section we evaluate and compare the performance of ordinary AODV for WMN with AODV routing protocol for WMN using GA and secure transmission by using NS-2.

4.1 Simulation environment

In our simulation, the propagation model is two ray ground reflection models and the MAC protocol is IEEE 802.11. The simulation parameters are listed in the below tables. The network coverage area is a 1000 m· 1000 m square with 50 mobile nodes. There are 20 constant bit rate CBR traffic resource distributed over the network. The CBR data packets are 512 bytes, and the sending rate is 4 packets per second. Simulations run for 300 seconds.

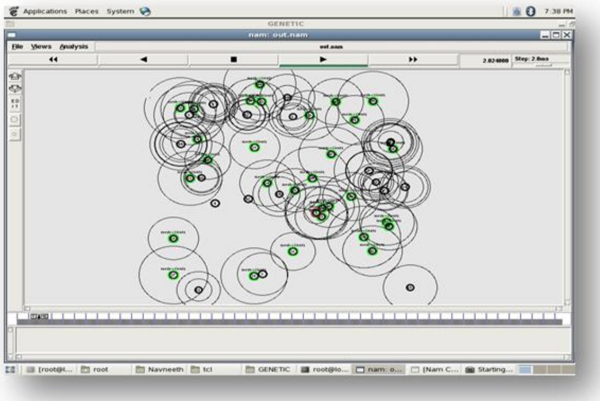

Fig 1: Source node sending packet to destination

4.2 Simulation Results

Our experiments verify that the proposed protocol can, indeed, successfully cope with a high number of adversaries, while operating only in an end-to-end manner. Moreover, we find that with limited overhead it is successful in delivering data, when compared to a protocol that uses no message dispersion. In our simulation, the total number of node in the network is fixed and it is 50 including mesh routers and mobile clients. We are comparing our algorithm efficiency in the context of variable number of mobile clients.

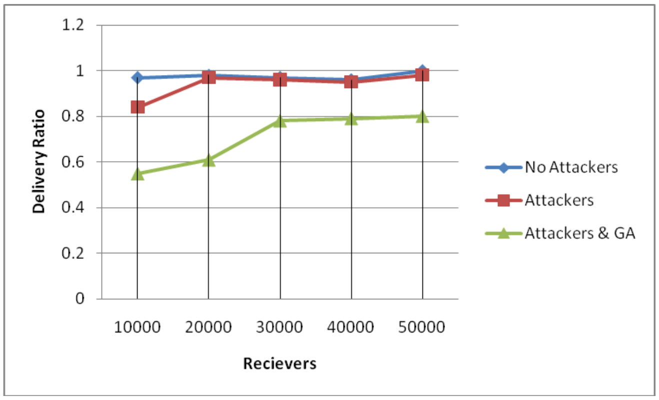

Fig 2: Packet delivery ratio

Fig 2 illustrates the comparison of packet delivery ratio, in which the comparison is done between three network types. First one is without attacker nodes, second one is with attacker nodes and the last one is, with attacker node using proposed algorithm. Simulation results shows that the packet delivery ratio of third type is more than the second because we use prevention of malicious nodes in routing path.

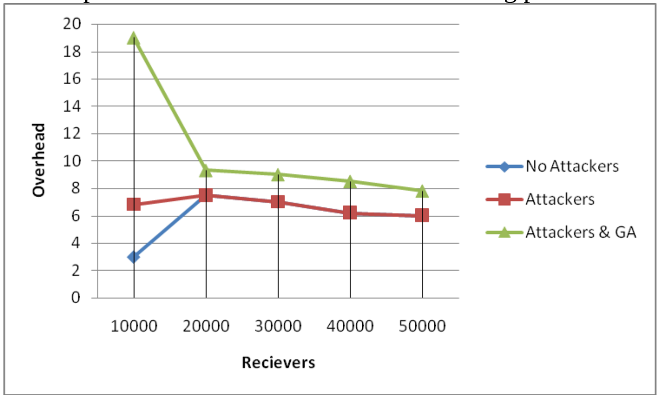

Fig 3: Overhead

Fig.3 illustrates the comparison of overhead in the networks. Initially there may be little more overhead in our protocol but it will be overcome in few seconds to give us a better result.

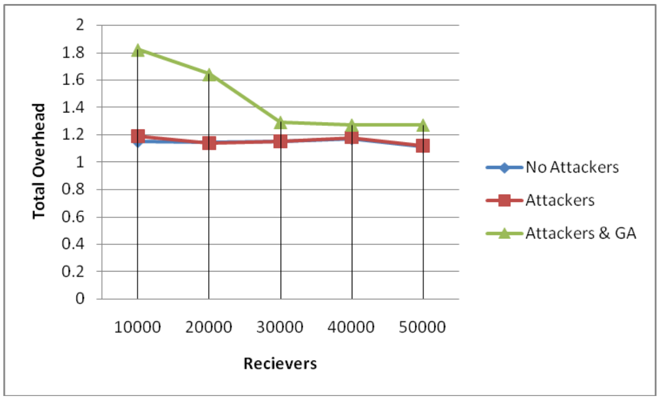

Fig 4: Total Overhead

Fig.4 illustrates the comparison of total transmission overhead in the networks. Here ,initially it is high but after some time our protocol starts approaching the minimum overhead, which is equal to network where attacker nodes are absent.

5.Conclusion

Genetic algorithm is used in the proposed system to find the optimal path from the route discovery. These optimal path are not only shortest path, it is the shortest end to end delay path and that can transmit more amount of data that can be sent in the network. Multi path routing is used to deliver message shares across the network, so that in the event that a small number of shares are compromised, the secret message as a whole will not be compromised. Our proposal takes advantage of topological and transmission redundancies and utilizes feedback, exchanged only between the two communicating end-nodes. This way, even under highly adverse conditions it remains effective. We simulate our proposal using NS2 and obtain the result that shows the packet drop ratio is very low and packets sent are high than the existing system.

References

[1]Ashish Raniwala, Kartik Gopalan, Tzi-cker Chiueh,*Centralized Channel Assignment and Routing Algorithms for Multi-Channel Wireless Mesh Networks*.In ACM SIGMOBILE Mobile Computing and Communications Review (MC2R), April 2004.

[2]Ashish Raniwala, Tzi-cker Chiueh,*Architecture and Algorithms for an IEEE 802.11 based Multi-channel Wireless Mesh Network*.In proceedings of IEEE InfoCom, March2005.

[3]Murali Kodialam, Thyaga Nandagopal.*Characterizing the capacity region in multi-radio multi-channel wireless mesh networks*.In proceedings of Mobile Computing andNetworking. August 2005.

[4]Mansoor Alicherry, Randeep Bhatia, Li (Erran) Li.*Joint Channel Assignment and Routing for Throughput Optimization in Multi-radio Wireless Mesh Networks*.In proceedingsof Mobile Computing and Networking. August 2005.

[5] Ana Paula R. da Silva, Marcelo H. T. Martins, Bruno P. S. Rocha, Antonio A. F.Loureiro, Linnyer B. Ruiz, Hao Chi Wong,*Decentralized intrusion detection in wirelesssensor networks,*In Proceedings of the 1st ACM international workshop on Quality ofservice and security in wireless and mobile networks (Q2SWinet 2005), pages 16-23,October 2005.

[6] Yi-an Huang, Wei Fan, Wenke Lee, Philip S. Yu,*Cross-feature analysis for detecting ad-hoc routing anomalies*. Proceedings.23rd International Conference on DistributedComputing Systems, Pages: 478 487, May 2003.

[7] Hao Yang, Shu. J, Xiaoqiao Meng, Songwu Lu,*SCAN: self-organized network-layer security in mobile ad hoc networks*, Appears in: IEEE Journal on Selected Areas inCommunications, Volume: 24, Issue: 2, pages 261- 273, Februry 2006.

[8] L. Badia, A. Botta, and L. Lenzini*,“A genetic approach to joint routing and link scheduling for wireless mesh networks,” Ad Hoc Netw.*,vol. 7, no. 4, pp. 654–664, Jun. 2009.

[9] H. Cheng, N. Xiong, G. Chen, and X. Zhuang*, “Channel assignment with topology preservation for multiradio wireless mesh networks,”J. Commun.*,vol. 5, no. 1, pp. 63–70, Jan. 2010.

[10]Richard Draves, Jitendra Padhye, and Brian Zill,“*Routing in Multi-Radio, Multi-Hop Wireless Mesh Networks*,”High throughput route selection in mult-rate ad hoc wireless networks. Technical report, Johns Hopkins University, 2009.

[11] Sharad Sharma, Shakti Kumar, Brahmjit Singh, “Hybrid Intelligent Routing in Wireless Mesh Networks: Soft Computing Based Approaches”, I.J. Intelligent Systems and Applications, 01, pp. 45-57, 2014.

Biographies

R. KALPANA is currently working as Associate Professor in the Department of Computer Science and Engineering at Pondicherry Engineering College, Puducherry, India. She received her B.Tech. degree in Computer Science and Engineering from Pondicherry University, Puducherry, India in the year 1996 and M. Tech. degree in Computer Science and Engineering from Pondicherry University, Puducherry in1998. She joined as Lecturer in Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry in the year 2000. Subsequently she was promoted as Assistant Professor in the Department of Computer Science & Engineering, Pondicherry Engineering College, Puducherry in the year 2007 and elevated as Associate Professor in the year 2010. Her areas of interest include Parallel Computing Systems, High Performance Computing and Distributed Computing. She has published research papers in International Journals and Conferences.

KUMAR NAVNEET was a student in the Department of Computer Science and Engineering at Pondicherry Engineering College, Puducherry, India. He received his M. Tech. degree in Computer Science and Engineering specialized in Distributed Computing Systems from Pondicherry Engineering College, Puducherry