Optimization and Analysis of Internet Gateway Deployment Problem with Load Balancing in WMN

Vishal Khatri, Research Scholar, Department of CSE, CMJ University.Shillong (Meghalaya)
Dr. P. K. Vashishtha, Supervisor , Dept. of Computer Science & Engineering ,CMJ University.Shillong (Meghalaya)

Abstract:

Internet Gateway problem is the fundamental problems for Wireless mobile networks (WMN). We provide an analytical framework under two IGW oriented architectures. The node throughput capacities of IGW and MR are analyzed and defined. To incorporate the effects of co-channel interference, we proposed three interference models for our IGW deployment approaches.The integration of WMNs with different systems, for example, the Internet, cell, IEEE 802.11, IEEE 802.15, IEEE 802.16, sensor systems, and so forth., can be practiced through the entryway and connecting capacities in the work switches. Work customers can be either stationary or portable, and can frame a customer work organize among themselves and with work switches. WMNs are foreseen to determine the impediments and to significantly improve the presentation of specially appointed systems, remote neighborhood (WLANs), remote individual territory systems (WPANs), and remote metropolitan region systems (WMANs). They are experiencing fast advancement and moving various arrangements. WMNs will convey remote ser-indecencies for an enormous assortment of uses in close to home, nearby, grounds, and metropolitan regions. Regardless of ongoing advances in remote work organizing, many research difficulties stay in all convention layers. This paper introduces IGW oriented network architecture of a WMN and the load balancing between IGW domains are important in determining the network performance.

Keywords:

Internet Gateway; Ad hoc systems; Wireless mobile networks; Load Balancing; Security.

Introduction

An **Internet gateway** is a network "node" that connects two different networks that use different protocols (rules) for communicating. ... If you have a Wi-Fi connection at home, your **Internet gateway** is the modem or modem/router combination that you're ISP provides so that you connect to the **Internet** through their network. Gateways can take several different forms from hardware to software - including routers and computers - and can perform a variety of tasks. These can range from passing traffic to the next 'hop' on its path to filtering traffic, proxies, or protocol translations. Because gateways are, by definition, at the edge of a network, they are often combined with firewalls, which keep out unwanted traffic or 'foreign' computers from a closed network.For Internet connections at home, the Internet gateway is usually the Internet Service Provider (ISP), who, in this case, offers access to the entire Internet through its own network. If you have a Wi-Fi connection at home, your Internet gateway is the modem or modem/router combination that your ISP provides so that you connect to the Internet through their network.If your Internet gateway is a computer server, which is more likely in an office or business situation, it acts as a firewall and a proxy server. A firewall, as discussed earlier, keeps unwanted traffic and outside computers out of a private network. A proxy server makes sure that the actual server can handle your online data requests.Routers are often Internet gateways. They are a piece of hardware that essentially connects your computer to the Internet. In home networks, it is usually something that comes with software you can install on one computer and then connect other computers to as well. Then everyone connected to your router can connect to the Internet through your ISP. While a router can be connected to more than two networks at a time, this is usually not the case for routers used at home. When you send a computer through your computer, your router will figure out the next

destination of the data depending on the networks it's connected to. This is how a router acts as a gateway because it controls the path through which the information is sent and retrieved.

Issues & Challenges:

Wireless telecommunications is the transfer of information between two or more points that are not physically connected. Distances can be short, such as a few meters for television remote control, or as far as thousands or even millions of kilometres for deep-space radio communications. It encompasses various types of fixed, mobile, and portable two-way radios, cellular telephones, personal digital assistants (PDAs), and wireless networking. Other examples of wireless technology include GPS units, Garage door openers or garage doors, wireless computer mice, keyboards and H WMN is becomes very popular in wireless networking technology for create the network connectivity for

home networking, community etc. It is necessary to efficient design and secure communication protocol for the WMN. The several parameter are used in the field of security like detect threats, black hole, colluding miserly, authentication, DOS attacks etc.The various security challenges related to WMN like firstly, WMN level to active attacks, Passive attacks and message distortion. The active and passive attacks like integrity,authentication, availability, non-repudiation and confidentiality. Secondly, we know that WMN is dynamic self organization and self configured. It means that all nodes in mesh network design is authenticate established and maintain network connection [4]. Some security attacks and research issues are described in Table 2.

Physical Layer

The challenges of physical layer are not different to other technology. In WMN, the physical layer should be Reliable. At the Radio transmission, several spread spectrum like Code Division Multiple Access (CDMA), Frequency Hopping Spread Spectrum (FHSS), and Orthogonal Frequency Division Multiplexing (OFDM) and Ultra-Wide Band (UWB) increase reliability. So it can accomplish much better spectrum utilization and feasible frequency planning for WMN. The common folds issues in physical layer are: Firstly, it is necessary to more recover the transmission rate performance at physical layer technique. According to the scope of multiple antenna system have been reached Secondly, it can provide the advanced higher features provided by higher layer protocol. Physical layer, and MAC layer. It can makes hardware design more challenging [15].

Data link Layer

Data link layer (DLL) is second layer, in which to access and transmission in the radio channel. The many attacks are found in DLL like traffic flooding, collision, rate limitation is resolved by Enhanced Distributed Channel Access (EDCA). In which author proposed the QOS function this layer is main design for MAC protocol. The multiple MAC protocol means to receive the data from more than one channel for one user transmission. So it can increase the overall performance and MAC layer for smart antenna part for 3G. The advantage of smarter MAC layer are increase link budget, reduced transmission power, increase reliability, layer transmission range. The different types of antenna at DLL are: passive eavesdropping, MAC address spoofing, jamming, replay, unfairness in allocation and partial matching. Following issues at DLL WMN are scalable Mac, MAC physical Cross Layer Design and network integration in Mac layer.

Network Layer

In generally the main function of network layer is transfer the packet from source to destination during multiple hops. According to these respect, WMN is different from MANET, Ad hoc network and 3G systems. In any technology routing protocol is very important factor but in WMN it is differentbetween failure and success. [15]. The different types of routing protocol are multipath

routing, Multi radio routing, Hierarchical Routing, and Geographic Routing. The main issues at Network Layer are as follows: better performance, scalability, Efficiency.The two types of attacks in network layer: Control packet Attacks and Data packet Attacks. Both these attacks could be either in active or passive. Rushing attacks, wormhole attack, Black hole attack, Sybill attacks are found in Control Packet Attack. Passive eavesdropping attacks found in data packet.

Transport Layer

According to previous knowledge no protocol has been planned in particular WMN. Transport protocols are available for ad hoc networks. Such as different type of attacks are: SYN flooding attack, Desynchronized attack and Session Hijacking attacks. The open issues are to resolved the cross Layer solution network asymmetry and adaptive TCP.

Application Layer

At the Application Layer, it requires a complete knowledge of the communicating applications as well as concession all the lower layer, the many applications are supported by WMN storage and sharing, information exchange across multiple wireless networks. The following attacks are found at application like Flooding attacks, Snooping attacks, Malwares, viruses and worms.

Comparative Analysis of Different Load Balancing Approaches to solve IGW Problem:

Total Network Load Based approach:

In this approach, at first, all the sinks are associated to their nearest gateway in terms of routing metric using the Nearest Gateway (NGW) solution [4]. Now NGW may result some congested domains. In such condition, it is very much necessary to balance the load of the network by reducing the load of the congested domain. Otherwise it may cause packet loss. Each of the domains has its own capacity. The locality of traffic also affects the capacity of network [13, 14]. The total load of the domain is the summation of the demand of each sink in the domain. If the total load of the domain exceeds the capacity of that domain, the domain is found to be overloaded. The overload is calculated as the difference between the total load of the domain and the capacity of that domain. The overload of the whole network is the summation of the overload of each domain of the network. At first the algorithm starts to assign all the sinks to their domains using the nearest gateway solution. Now if a domain is found to be overloaded, the sinks under the domain is checked in descending order of distance to their NGW to reroute their flow to other domain. Using this method, the preference to the border sinks are given. Now after choosing a sink, the neighboring domains are checked in ascending order of distance from that sink. To switch the sink, it is necessary that the overload after the switch must be less than the overload before the switch. If the overload is decreased it checks the cost of switching. This prevents the establishment of long paths. If the cost is below a certain threshold, the flow of the sink is rerouted to the desired domain.

Adaptive Situation-Aware Metric Based Approach:

In this approach, an Adaptive Situation–Aware (ASA) metric [5,11,12] is calculated . This approach selects the path having good performance and decrease the effects caused due to the interference. It also keeps track of the load balance of the network. There are three steps of this approach. In first step, the ASA metric cost of the channel is calculated. ASA metric considers the parameters like the channel access overhead, protocol overhead, bits of test frame, transmission rate etc. and calculates the metric on the basis of these parameters. Then the total ASA metric cost of the path is calculated. The path having minimum ASA metric cost is chosen. Now the chosen path may have uneven ASA metric cost. So, to decrease the packet loss and also to achieve load balance, the concept of Max-flow Min-cut is used in the second step. Several paths may have the same ASA metric cost but the distribution of cost of the link may be different. It may cause congestion of packets at any node. To avoid this situation, the concept of Max-flow Min-cut is used. Using this concept, it can select such a path in which the load distribution is uniform and

thus the packet loss is reduced. Now in the third step the load balancing algorithm is executed. Here a time threshold is set to update the metric cost periodically. If the current time is greater than the threshold, again the update of the ASA metric cost is to be done. After update, if any other path is having the minimum ASA metric cost, the flow is routed to that path. Otherwise, the flow is continued to the current path.

Partitioning Based Approach:

The partition-based load balancing (PLB) approach does single path routing in multi-sink wireless mesh networks. The algorithm applies load balancing in between partitions within partitions [7]. It is considered that a node may have multiple downlinks but only one uplink. The node having more than one downlink is termed as division point. Each node has a cumulative load which is the sum of the weights of all nodes of the sub-tree. The load balancing algorithm consists of three phases. They are: Load Adaptive Clustering phase (LAC), Inner Domain Load Balancing (IDLB), and Outer Domain Load Balancing (ODLB). IDLB performs the load balancing within each domain. It balances the load among the downlinks towards node including a sink node. LAC partitions the whole network into domains. It uses hop-count to cluster the network into domains. There is a timer in a node and each performs clustering at its own scheduled time. The back-off time is used to slow down the clustering speed of the overflowing domain. For clustering operation, a node may be in one of the 4 phases: PENDENCY, EXPANSION, OVERFLOW and SETTLEMENT. PENDENCY is the first phase which denotes that the assignment of the node to any domain is not done yet. EXPANSION is the state, when a node is preparing for clustering. OVERFLOW is set when a newly added node's weight is larger than the available bandwidth of the top sub-link. SETTLEMENT indicates the completion of the clustering. ODLB performs load balancing across the domains. It resolves the unbalanced load condition that the IDLB cannot deal with via inter-domain load balancing.

Responsive on-line load-balancing Approach:

The approach Responsive On-line Gateway Load Balancing focuses on the centralized approach [6] of gateway load balancing. The gateway selection is done centrally. There is a controller to monitor the whole network. The communication between controller and gateway is done through the wired network. Centralized gateway selection approach calculates routes between every active source-destination pair. Here the current demand of each node is assumed to be known, but it is not specified that how this information is known. At any one time, a flow can be served by only one gateway. A gateway's native domain is the set of nodes closest to it according to the routing protocol metric. The controller takes the information of current set of flows and calculates a fast gateway selection algorithm. Then it calculates the summation of the loads served by the gateway. In WMN, path is established between gateways and sinks. These paths are known to the controller. Now the distance of a node to a set of nodes (domain) is the minimum distance from that node to a node among the set of nodes(domain). The distance from a path to a set of nodes is the arithmetic mean of the distance of the nodes of the path from the set of nodes. The cost of a path from a gateway to a sink is the negative distance of the path to nodes which are not in the native domain of that gateway. Now, to solve the multi-objective problem, the first objective is to minimize the maximum number of flows through the gateway. The second objective is to avoid interference by minimizing the cost of the paths. To reach a sink, it chooses the path in the ascending order of the cost. The algorithm considers the sinks which are not locked. The sinks, at first, are not assigned to any gateway. Then a sorting is done using the sink comparison function. So the list of unlocked sinks is found. For each unlocked sink the algorithm chooses the least loaded gateway as its current gateway. If there exists more than one least loaded gateway the one with lowest cost to reach is chosen. Thus the algorithm is executed to balance the load of the gateways.

Diffusion based Distributed Load Balancing Approach:

In this approach, a load balancing metric is defined in terms of load and capacity. A fairness index (β)[8] is calculated from the matrix.[9] The value of β ranges from 0 to 1.Higher values indicates more fairness in load distribution in WMN. A fairness of 1 indicates a perfect balanced utilization. This approach tries to improve fairness index β. If β of a domain reaches below some threshold, then load-balancing process is invoked. Here three different diffusion algorithms are implemented. Diffusion describes the spread of particles through random motion from regions of higher concentration to regions of lower concentration. Firstly,the load balance index is defined among Internet Gateway (IGW) service domains. To take heterogeneity into account the bandwidth utilization ratio is defined, which is the ratio of load to the capacity. Then the fairness index in heterogeneous WMN is defined. In this load balancing scheme, the traffic load of each of the domain is measured. Each IGW calculates the traffic load value in its domain by monitoring the amount of the flow of traffic through it during a given time window. Then the local load fairness index is calculated. If the local load fairness index is less than threshold, the load balancing algorithm is calculated. The three diffusion algorithms are: Basic Diffusion Algorithm, Search Unbalance Domains Diffusion Algorithm and Fast Diffusion Algorithm. The Basic Diffusion Algorithm calculates taking the neighboring domains. It calculates the local traffic load. In Search Unbalance Domain Diffusion Algorithm it uses the dynamic load balancing strategy. It not only compares the traffic load between the local load averages with neighbors, also tries to minimize the maximum load difference between any two neighboring domains. It is more improved than the first one. The third one is Fast Diffusion Algorithm. It consists of two phases. In the first phase, the local load average of domain is calculated. In the second phase of the algorithm, the similar strategy as in Search Unbalance Domain Diffusion Algorithm is used to minimize the maximum difference among neighboring domains. It can overcome the shortcomings of the previous two algorithms. Also it can achieve the load balancing faster than the previous algorithms.

Variance Based Approach:

In this approach [9] the mesh network is described as communication graph G=(V,E) ,where $V = \{v_1 , \ldots , v_m , \ldots , v_n \}$ is the set of mesh nodes ($n \geq m \geq 1$, n is the number of mesh nodes, m is the number of gateway nodes, and mesh nodes from v_1 to v_m are gateway nodes),and E is the set of links $l_{i,j} = (v_i,v_j)$. Mesh node is linked with other mesh nodes within the communication range.The routers choose their nearest gateways by shortest path routing (SPR) algorithm. Then load of each gateway and variance of the load on gateway nodes is calculated. The algorithm searches for the node whose variance is least and path length is below a threshold value. This process continues until the node reaches to a gateway node.

Probabilistic Approach:

In this approach simulated annealing technique is used. It reroutes the flow of Mesh Router (MR) from an overloaded domain to an underutilized domain. Here a fairness index (β) and load balance index (β') is used. After the adjustment of the load, the network goes to a stable state having the better fairness of the traffic loadMR is considered as the bordering node, which is able to connect to the multiple IGWs. The two domainsare called neighboring domains if there exists some bordering nodes between them. The load balancing is achieved by migrating the flows of the bordering MR from one IGW domain having higher load to the adjacent domains. The effect of the load is reflected from the load balance index (β'). The MR is selected using two basic methods: random selection and the greedy selection. But in some conditions, the intermediate migration is also taken which doesn't increase the balance index. But it is useful to achieve the global maximum load balancing. This simulated annealing is a probabilistic search method which can be used in wide range of areas. This method produces more optimal solution than the iterative technique. Though the balance index sometimes is not increased, the nodes may associate with neighboring domains properly. The MRs doesn't violate the capability constraints in time of migration.

CONCLUSIONS

The paper discusses different approaches of load balancing in Wireless Mesh Network. As the capacity of the link is limited, the gateways turn into bottleneck which causes congestion in the network. The observation reflects that in most of the cases, the load balancing is done through gateways. But the cost of the link is not considered much. It is also very important to keep uniform flow through the links. The link capacity also needs to be considered while balancing the load of the network. Otherwise links will be congested and packet loss will be high. To improve the network performance, path load balancing is as important as gateway load balancing. Link quality can also be taken into account to route the flow of the sink in order to provide Quality of Service to the mesh clients. Moreover, works may be done to integrate the link quality with domain capacity to balance the load of Wireless Mesh network.In this dissertation we investigated the authentication and key establishment schemes for wireless networks.WMN is a self healing, self organized and self learning network. There are many advantage of WMN like multiple interface, increased reliability, multiple radio frequencies, low deployment cost, self organization and self configuration but there are also some security challenges and issues. This paper discusses the security requirements, threat, challenges and issues of WMN. Now WMN technology facing multiple problems related to security which requires the consideration in the development of efficient wireless network. We provide two distributed authenticated key agreement schemes for efficient mutual authentication.

REFERENCES:

[1] Yan Zhang, JijunLuo, HonglinHu .WIRELESS MESHNETWORKING: Architectures, Protocols and Standards, AuerbachPublication, 2006.

[2] I.F. Akyildiz, X. Wang, and W. Wang, "Wireless mesh networks: a survey,"Computer Networks Journal (Elsevier), March 2005., vol. 47, no. 4, 2005.

[3] DeeptiNandiraju, Lakshmi Santhanam, NageshNandiraju, and

Dharma P. Agrawal, "Achieving Load Balancing in Wireless Mesh Networks Through Multiple Gateways", Mobile Adhoc and SensorSystems (MASS), 2006 IEEE International Conference , On page(s): 807- 812 on Oct. 2006.

[4] Juan J. Gálvez, Pedro M. Ruiz, Antonio F. G. Skarmeta , "A Distributed Algorithm for Gateway Load-Balancing in Wireless Mesh Networks", 1st IFIP Wireless Days (2008) , Publisher: Ieee, Pages 2008

[5]] Guan-Lun Liao, Chi-Yuan Chen, Shih-Wen Hsu, Tin-Yu Wu, Han-Chieh Chao , "Adaptive Situation-Aware Load Balance Scheme forMobile Wireless Mesh Networks", Computer CommunicationsWorkshops (INFOCOM WKSHPS), 2011 IEEE , On page(s): 391 - 396 ,10-15 April 2011.

[6] Johnston D, Walker J.2004. Overview of IEEE 802.16 Security. IEEE Security and Privacy: 2(3): 40-8.

[7] Zhang Y, Fang Y. ARSA.2006. An attack- resilient security architecture for multi-hop wireless mesh network. IEEE journal on selected Areas in communications: 24(10): 1916-28.

[8] Yan Y, Cao J, Li Z. 2009. Stochastic security performance of active cache based defense against dos attacks in wireless mesh network. In: Second International Conference on Advances in mesh networks (MESH 2009): P P: 30-6.

[9] Ren K, Yu S, Lou W, Zhang Y.2010. PEACE: a novel privacy-enhanced yet accountable security framework for metropolitan wireless mesh networks. IEEE Transactions on parallel an Distributed Systems: 21(2):203-15.

[10] Frank A, Z, Sebastian R, Albert B.2011.Security analysis of wireless mesh backhauls for mobile networks, Journal of Network and Computer Applications. Elsevier, 432-442.

[11] Kuhlman D, Moriarty R, Braskich T, Emeott S and Tripunitara M. 2007. A proof of security of a mesh security architecture. Technical Report, IEEE press: 2007.

[12] Zorana B, Davis F, Jose M,M, Juan C V, pedro M, Alvaro A, Juan M. G. Elena. R. Javier B, Daniel V, iOctavio N.T.2011. Improving security in WMNs with reputation systems and self-organization Maps. Journal of network and Computer Applications (2011), 455-463.

[13] Sen J.2009. A survey on wireless sensor network security. International Journal of Communication Networks and Information Security, 59-82.

[14] Hizbullahkhattak, Nizamuddin, FahadKhursid, "Preventing Black and Gray hole attack in AODV using optimal path and routing hash"

[15] G. Indiriani, Dr. K. Selvakumar, "Intrusion detection and defense mechanism for packet replication attack over MANET using Swarm Intelligence," pattern recognition, informatics and mobile engineering.

[16] SapnaGambhir and Saurabh Sharma, "PPN: Prime Product Number Based Malicious node Detection scheme for MANETs" International advance computing conference (IACC).