Journal of Information Systems and Communication
ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, 2012, pp.-210-214.
Available online at http://www.bioinfo.in/contents.php?id=45

PAIRS: ALGORITHM FOR SECURE HETEROGENEOUS WIRELESS NETWORKS

SUMAN[1*], SUKHDIP SINGH[2], PATEL R.B.[3] AND PARVINDER SINGH[4]

Dept. of Computer Sc. & Engg., Deenbandhu Chhotu Ram University of Sc. & Tech., Murthal, Sonipat, Haryana, India.
*Corresponding Author: Email- [1]suman2222@yahoo.com, [2]sukhdip_sangwan@rediffmail.com, [3]patel_r_b@yahoo.com, [4]parvinder23@rediffmail.com

Received: January 12, 2012; Accepted: February 15, 2012

Abstract- Ever increasing security threats such as intrusion detection, secure routing, key establishment and distribution, and authentication could harm and affect the feasibility of heterogeneous wireless networks(HWN).To reduce the probability of packet capturing and ensure greater protection from outside attacks in HWN, we present a multi parameter based algorithm PAIRS (Periodic Adaptive and Intelligent Route Selection).This algorithm is intelligent and adaptive as it can alter it's decisions to incorporate changes in link and node parameters . PAIRS selects best route using ANFIS (adaptive neuro-fuzzy inference system) periodically. PAIRS effectively balance overall load of network and prevents denial of service (DoS) attack by offering improved resource management. It also reduces congestion in network by diverting the traffic on alternate routes. In this paper, we have analyzed the performance of PAIRS in terms of network throughput.

Keywords- Heterogeneous wireless networks (HWN), security, route selection, neural network (NN), (adaptive neuro-fuzzy inference system) ANFIS, fuzzy logic, intelligent, adaptive.

Citation: Suman, et al. (2012) Pairs: Algorithm for Secure Heterogeneous Wireless Networks. Journal of Information Systems and Communication, ISSN: 0976-8742 & E-ISSN: 0976-8750, Volume 3, Issue 1, pp.-210-214.

Introduction

Heterogeneous wireless networks (HWN) provide anytime and anywhere connectivity to the mobile users without much concern for the background technology used for maintaining and securing connectivity. HWN requires new concepts and approaches to deal with the challenges posed by integration of technologies. Due to this reason, HWN have gained much attention of researchers over last few years.

Security is given much emphasis in computer and network systems around the world. [1] present an overview of standardization activities focusing on the network security architectures and a survey of security threats on 4G networks. Many security threats can cause unexpected service interruption and disclosure of information in heterogeneous 4G network. The reality of ever increasing security threats such as intrusion detection, secure routing, key establishment and distribution, and authentication which could harm and affect the feasibility of HWN is a significant and timely area of research. Although many researchers are designing new security architectures for 4G, but still much more need to be done.

Fuzzy logic systems and neural network classifiers are good candidates for pattern classifiers due to their non-linearity and generalization capabilities. Fuzzy logic can represent human knowledge as fuzzy rules and can be used to develop cost-effective approximate solutions. These solutions can be used for evaluation of services offered by different networks and to infer crisp output value [2]. A neural network (NN) is a massively parallel distributed processor made up of simple processing units, which has a natural propensity for storing experimental knowledge and making it available for future use. NN acquires knowledge through a learning process (supervised or unsupervised) and synaptic weights are used to store the acquired knowledge. Once a NN is trained, it can recognize unseen patterns.

To overcome the challenge of packet capturing and provide protection from outside attacks in HWN, we present a multi parameter based algorithm - PAIRS (Periodic Adaptive and Intelligent Route Selection). It uses designed and trained ANFIS (adaptive neuro-fuzzy inference system) to select the best available route periodically. PAIRS is intelligent, adaptive and reduces congestion in network. This algorithm effectively balances overall load of the network and prevents DoS attack by offering improved resource management. We have analyzed the performance of PAIRS in terms of network throughput.

Related Work

Providing adaptive and intelligent security solutions for open and heterogeneous environment is very difficult. Previous research on security issues in HWN can be divided into three main categories, namely, authentication, collaboration incentives, and denial of service (DoS) prevention (summarized in [3]).

DoS prevention falls into two categories: improved resource management [4] and avoidance mechanisms [5]. For low-capacity networks (eg. ad-hoc and sensor) improving resource management mechanisms can help reduce the disparity when they are connected to high-capacity networks (eg. wired and fiber-optic), thus leading to increased heterogeneity in the network. Increased congestion and saturation in heterogeneous networks leads to more and more DoS disruptions, which increases with increase in disparity of resources between different parts of the network. Therefore, DoS prevention must be addressed explicitly in context of the next generation networks.

To deal with DoS, a probabilistic route selection algorithm that traces attacker’s real origin is presented in [6]. Quality of service (QoS) aware path selection scheme to estimate required bandwidth ratio is presented in [7]. This ratio is based on the QoS requirements of target service and SINR of each path. The proposed scheme can select multiple/single optimal path to satisfy the QoS requirements among dynamically changing HWN.

In [8], NN based optimal path selection algorithm is presented for managing multihomed hosts attached to HWN. In [9], an adaptive and efficient routing protocol for integrated cellular and ad-hoc heterogeneous network with flexible access (iCAR-FA) is presented. [9] also presents detailed numerical analysis on route request rejection rate.

In [10], novel load-aware route selection algorithm, (LARS) is presented. In this approach each mesh node is allowed to distribute the traffic load among multiple gateways for uniform utilization of Internet connections leading to improved network capacity. However LARS design does not consider end-to-end delays in the selection of feasible network paths.

In [11], heterogeneity of nodes and delay is considered during route discovery to discover resource-rich routes. Paths that contain more capable nodes are utilized, thereby avoiding resource-poor nodes. This paper does not focus on the issue of choosing proper delay value for unknown network.

In [12], a generic and scalable security management service which scales with increasing diversity of network techniques and applications is proposed for inter domain communication of heterogeneous networks.

In [13], a flexible cryptography-based approach is presented for establishing trustworthiness between multi-hop mobile nodes using infrastructure supported authentication. Generalized multi-hop security protocol (GMSP) combines mobile IP and ad hoc security schemes to achieve an effective route discovery protection in accordance with anti-integrity, impersonation for generalized heterogeneous multi-hop networks. This protocol implements security in four steps namely registration for single hop mobile nodes, registration for multi-hop mobile nodes, routing security between base station and any mobile node, and security of the routing between any two mobile nodes.

Periodic Adaptive and Intelligent Route Selection

Attacks on HWN have become much more adaptive with passage of time. To deal with these attacks, networks should be able to adjust their security provisions and sophistication levels rapidly and intelligently.

Transmitting packets on same route might increase the risk of packet capturing in HWN. Our algorithm PAIRS reduce packet capturing by forwarding packets on different routes periodically. Since the route for packets is not known in advance, attacker can not launch either an active or passive attack.

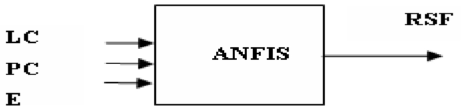

Fig. 1- Designed ANFIS for PAIRS

ANFIS with three inputs and one output is designed to rank different routes based on value of route selection factor (RSF). Training data is carefully chosen for tuning of training vector of ANFIS in Fig. (1) , so that it can well identify parameters and rules and give reasonable performance [14]. PAIRS use ANFIS to select route with highest RSF for packet transmission at any point of time. ANFIS once trained can calculate result for any value of input data using its stored knowledge, thus making PAIRS more intelligent.

RSF considers resource availability including processing power, link capacity, and battery life of nodes falling on the route under consideration. This effectively balance overall load of the network and prevents DoS attack by offering improved resource management. RSF considers the link capacity of route under consideration, leading to reduction in network congestion. PAIRS can alter its decision to incorporate changes in link and node parameters, making it adaptive at the same time.

A) Assumptions

The following assumptions are made to select best route using PAIRS

1. At any point of time, different nodes in network have different power backups and processing capabilities.
2. Links in network differ in link capacities / data rates.
3. All nodes maintain a routing table showing updated routes to all other nodes in the network.
4. All nodes in network have exactly D neighbors i.e. degree of network is D.
5. Arrival rate λ i.e. mean number of arrivals per unit time is same for all links.

Inputs to ANFIS

1) **LC**-It gives the current available bandwidth of link under co sideration. Lower value of LC signifies that large amount of traffic is currently passing through this link. Further increase in number of packets may lead to increase in congestion and decrease in throughput of network. So, higher the value of LC more is the probability of that route being selected for packet

forwarding. In designed ANFIS, range of LC is taken from 0 to 1.

$$LC = (Bt - Bu) / Bt \quad (1)$$

Where Bt = total bandwidth of network
Bu=used bandwidth of the link under consideration at given point of time
Even if link with low value of LC has two nodes on endpoint with high value of PC and E, choosing that link as part of route may degrade network throughput as it will put additional traffic load on the slow-speed link. It asserts that a link can not transfer data faster than it's remaining bandwidth. So LC has maximum impact on RSF and network throughput.

2) **PC**-It is related to current CPU usage of node under consider tion. PC is the measure of remaining processing capacity of node under consideration. Lower value of PC signifies that much of CPU capacity is currently being used for processing packets. Any further addition of packets to CPU may lead to congestion and this might degrade overall performance of network. So route having higher PC will be selected. In designed ANFIS, range of PC is taken from 0 to 100.

$$PC = (100 - CPUu) \quad (2)$$

Where CPUu =current CPU usage

3) **E**-It measures current battery backup of node under consider tion. Lower value of E signifies that node is running out of power. So it would not be appropriate to use that node for packet forwarding. In designed ANFIS, range of E is taken from 0 to 100.

Table 1-Notations

Symbol	Definition
LC	Current link capacity of link under consideration
PC	Current processing capacity of node under consideration
E	Current power of node under consideration
NP	number of packets after which new route is to be selected by using ANFIS(i.e. PAIRS is to be run)
TAR	Total number of times PAIRS is run in network
λ	Arrival rate ,Mean number of arrivals per unit time
AQD	Average queuing delay for all packets sent through the network from source to destination
S	Total number of packets offered to network
M	Average packet length in bits
B	Data rate on link in bits per second (varies for each link)
N	Total number of links in network
D	Degree of Network
K	Number of levels in network
T1	Average time taken for single iteration of PAIRS. It is calculated by taking average over 10 iterations.
Algo_time	Total delay caused by PAIRS(for total runs in network for S packets)
Gen_time	Time for generation of S packets using poisson distribution at source
PGT	Total time for generation of S packets using poisson distribution at source
PGT1	Time for generation of all bits of one packet at source
Throughput	Throughput of network when PAIRS is used to select best route periodically
Tot_time	Total time for transmission of all data packets from source to destination

PAIRS Algorithm

A source node transmits a packet to a neighboring node with which it can communicate directly. The neighboring node in turn transmits this packet to one of its neighbors, and so on until the packet is transmitted to its final destination. Each link that a packet is sent over is referred to as a hop; the set of links from the source to the destination is called a route or path. PAIRS is run on all nodes in the network that have some data to transmit
Single iteration of PAIRS is given below:

1. Node i that want to transmit packets will calculate RSF using ANFIS for next hops on all available routes to destination, where i= 1, 2, 3….D.
2. Route with highest RSF is selected for packet transmission by current node i.
3. Current node i resets its packet counter Pi=0.
4. Node i transmit packets.
5. If Pi <=NP go to step 4, else go to step 1.

Performance analysis for PAIRS

We will analyze performance of PAIRS by calculating throughput of network and the effect of node density on throughput. The delay used in calculation of total time has two components-average queue delay (AQD) and delay due to PAIRS.

A. Average Queue delay

Jackson's theorem is used to analyze a packet switched network as network of queues [15]. The theorem is based on three assumptions:

1. The queuing network consists of m nodes, each of which provides an independent exponential service.
2. Items arriving from outside the system to any one of the nodes arrive with a Poisson rate. In ANFIS, range of RSF is taken from -9.558 to 7.331.
3. Once served at a node, an item goes (immediately) to one of the other nodes with a fixed probability, or out of the system. Each packet represents an individual item. We assume that each packet is transmitted separately and, at each packet switching node in the path from source to destination, the packet is queued for transmission on the next length. The service at a queue is the actual transmission of the packet and is proportional to the length of the packet.

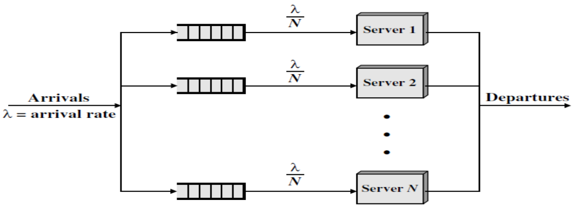

Fig. 2- Multiple Single Server Queues [15]

Multiple single server queue model of Fig. (2) is used to calculate AQD [15].

B. Delay due to PAIRS

At each level, PAIRS is run exactly (S/NP) number of times.

$$N = \sum_{L=1}^{L=K} (D \wedge L) \quad (3)$$

$$AQD = (1/S) \sum_{i=1}^{i=N} (M * \lambda i) / (Bi - (M * \lambda i)) \quad (4)$$

$$TAR = (K * (S / NP)) \tag{5}$$

$$A\lg o\_time = T1 * TAR \tag{6}$$

C. Throughput

Throughput is measured as total number of packets delivered from source to destination in given time. We consider only data packets ignoring acknowledgement packets for calculation of throughput of network when PAIRS is used for route selection.

$$PGT = Gen\_time + (S * PGT1) \tag{7}$$

$$Tot\_time = PGT + A\lg o\_time + AQD \tag{8}$$

$$Throughput = S / Tot\_time \tag{9}$$

Simulation

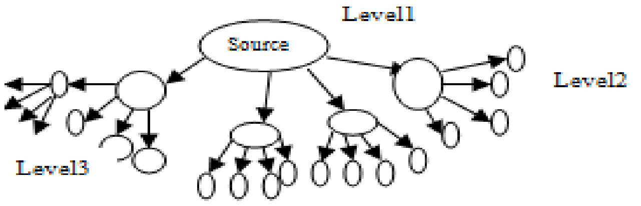

Fig. 3- Network with degree 4

For simulation we have chosen network shown in Fig. (3) with following value of parameters.
D=4, NP=100 packets,
M=2000 bits, S=1202 packets,
PGT1= 0.0002 s, λ =4,
K=1, 2…5,
B is generated as a random number in range 10000 bps to 54000000 bps.

Results and Discussions

We carried out simulation with above mentioned values of parameters and obtained following results.
PGT=0.3130s, T1=0.08193s

Table-2- AQD and throughput of network using PAIRS

AQD (ms)	N	K	Number of nodes=N+1	Throughput (%)
0.0010963	4	1	5	77
0.0086002	20	2	21	43.8
0.10861	84	3	85	30.6
0.80208	340	4	341	23.51
2.3	1364	5	1365	19.09

Values of AQD and throughput for different number of nodes in network are summarized in Table-2.

Variation of AQD with increase in number of links is plotted in Fig. (4). AQD is very less for single hop network and it increases with increase in number of nodes. Variations in AQD are random because it includes random variable B. Variation of throughput with increase in node density is plotted in Fig. (5). Throughput for single hop network using PAIRS is quiet good i.e. 77%. Throughput falls sharply for 2 hop network. For 3, 4 and 5 hop network throughput shows small decrease and finally it becomes nearly constant.

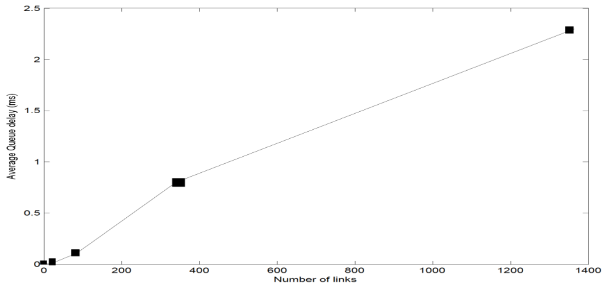

Fig. 4- Average queue delay Vs Number of Links

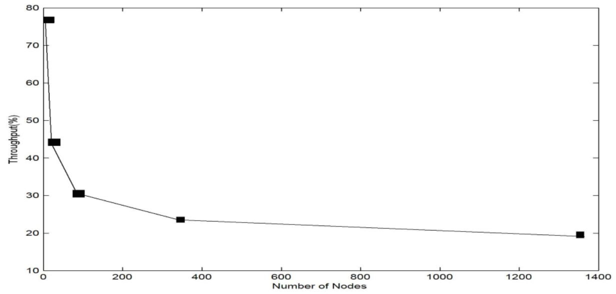

Fig. 5- Throughput Vs Node density

Conclusion

Route selection based on multiple parameters is a difficult task. We used fuzzy logic and artificial neural network to improve efficiency, performance and adaptiveness of yields. PAIRS an intelligent multi -criteria route selection algorithm for HWN selects best route among the available. It uses LC, PC and E to decide for new route and effectively balances power and resource utilization of HWN. PAIRS use ANFIS for ranking of different routes based on availability of resources on those routes. We analyzed the performance of network in presence of PAIRS and results obtained were quiet good.

PAIRS reduce packet capturing by forwarding packets on different routes periodically. It ensures greater protection from outside attacks for HWN. PAIRS effectively balances overall load of the network and prevents DoS attack by offering improved resource management. It also reduces network congestion by considering link capacity of routes in RSF calculation. PAIRS can alter its decision to incorporate changes in link and node parameters, making it adaptive at the same time. It uses ANFIS which once trained can calculate result for any pair of input data using its stored knowledge. This imparts more intelligency to PAIRS.

In this paper, we considered only data packets for calculation of throughput of network. In future, acknowledgement packets may be considered for traffic load calculation. Packet loss in network may be incorporated for more appropriate throughput calculations in future.

References

[1] Yongsuk Park, Taejoon Park (2007) *IEEE Globecom Workshop,* 1-6.

[2] Mikut R., Jakel J., Groll L. (2004) *Journal of Fuzzy sets and systems*.

[3] Evans J.B., Wang W., Ewy B.J. (2006) *International Journal on Security and Networks*, 1(2), 84-94.

[4] Bhatia R., Li L.E., Luo H., Ramjee R., Sanjoy P. (2006) *IEEE Transactions on Mobile Computing,* 5(8).

[5] Enck W., Traynor P., McDaniel P., Porta T.L. (2005) 11*th ACM conference on Computer and communications security* (CCS).

[6] Yim H., Kim T., Jung J. (2011) *IEEE International Conference on Information Science and Applications.*, 706-713.

[7] Shin-Hun Kang, Jae-Hyun Kim (2010)7*th IEEE/ACM conference on Consumer communications and networking conference*.

[8] Zifan Li, Tao Zhang, Chong Shen (2011) *IEEE Second International Conference on Intelligent Systems, Modelling and Simulation*, 344-349.

[9] Yumin Wu, Kun Yang, Jie Zhang (2006) *ACM international conference on Wireless communications and mobile computing*.

[10] Raffaele Bruno, Marco Conti, Antonio Pinizzotto (2009) *IEEE international symposium on world of wireless, mobile and multimedia networks and workshops*, 1-9.

[11] Ian D. Chakeres and Elizabeth M., Belding-Royer (2003) *Resource Biased Path Selection in Heterogeneous Mobile Networks. UCSB Technical Report*.

[12] Rohrer, Justin P. Sterbenz, James P.G., Wang Weichao (2007)*IEEE Military Communications Conference*, 1-6.

[13] Bin Xie, Srinivasan A.K.S., Agrawal D.P. (2006) *IEEE Conference on Wireless Communications and Networking*, 2(3), 634-639.

[14] Suman, Sukhdip Singh, Patel R.B., Parvinder Singh (2012) *ACM Conference on Security and Privacy in Wireless and Mobile Networks*.

[15] Queuing analysis, William Stallings (2000) *William-Stallings.com/Student Support.html*.