

Increasing QoS and Security in 4G Networks Using Cognitive Intelligence

Rajani Muraleedharan and Lisa Ann Osadciw
Department of Electrical Engineering and Computer Science
Syracuse University
Syracuse, NY 13244-1240 USA
1(315)-443-1319
{rmuralee/laosadci}@ecs.syr.edu

Abstract - Mobile networks have become an essential part of our day to day lives. The information shared requires secure communications with high reliability and quality-of-service (QoS). Hence, designing a 4G network to provide secure IP-based service by trading off constraints such as battery life, bandwidth and size to mobile users is a challenging task. In this paper, a cognitive framework using an evolutionary algorithm, Swarm Intelligence, is proposed. This framework uses a novel approach that utilizes a cost function that chooses the optimal parameters to provide an adaptive quality of service (QoS) based on the user's needs. This approach ensures interoperability and scalability between different modulation techniques in the physical layer and enhances security against Denial of Service attacks such as jamming attacks and signaling attack.

Index Terms - 4G, Cognitive Intelligence, Heterogeneous network, QoS, Security, Denial of Service, Swarm Intelligence

I. INTRODUCTION

The evolution of wireless networks has seen a tremendous impact on economy and is widely considered as a trend setter. Recent growths in wireless technology demand more security, reliability and still are cost effective 4G mobile networks. Since the first mobile network, there has been a rapid improvement in both technology and service to the users. Unfortunately, there have also been many issues that hinder the future of 4G applications, such as limited power, handoff [4], computation ability, bandwidth, size and cost. Thus researchers are working on 4G while the earlier 3G technology is still in the marketing phase.

In late 1980s, the industry witnessed the growth of 1G mobile communications where analog frequency modulation was used, whereas the 2G used digital communication technique using Time Division Multiplexing (TDM), frequency division multiplexing (FDM), code division multiple access (CDMA) or M-ary coding schemes. The 1G system was analog with bandwidth of 2.4kbps, and the 2G systems improved upon this up to 64kbps. Initially 3G mobile systems were designed to provide voice and paging service for interactive multimedia with coverage of 2Mbps. Thus, the main contribution of 4G to the mobile community is

combining heterogeneous network while facilitating both voice and data transfer with high quality-of-service (QoS). The QoS requirements for 4G include minimum delay (real-time data), minimum hand-off, minimum or no drop calls and controlled load balancing under high traffic intensity.

The main concern of any wireless mobile device is security in terms of data, hardware and user's privacy. Security breaches are often initiated either by the imposter or due to incorrect parameter settings. For e.g., user's mobile settings is often kept public or open, hence any intruder can access the data, and in another scenario where in spite of, good security features of the device, constant signaling attack [7] can lead to continual resource exploitation. In either case, the affected mobile user will be denied access irrespective of resource availability such as energy, channel availability, bandwidth. Thus 4G requires security features that balance the resource availability while achieving high QoS. Additionally, complex security algorithms or framework can be applied only if the mobile equipment (ME) has the available resource to support the operation.

The main security concerns of a 4G network are as follows,

- Integrity of the hardware, software, data and operating System (OS): Application Security
- Confidentiality, Integrity, Authentication and Authorization (CIAA) of data : Network Access Security
- User's identity, Confidentiality and authorization: User security [1,3]
- ME's location authentication and confidentiality: Network area Security
- Security against Denial of Service (DoS) attacks: QoS maintenance
- Tamper resistance: Physical Security

Among the above six features, tamper resistance is one which is often neglected and also assumed to be least vulnerable if complex algorithms are used to protect ME. In order to have a balanced security features, while maintaining interoperability and scalability among global mobile service a simple cognitive framework using swarm intelligence (SI) [9, 13] can be used.

The framework proposed in this paper helps in achieving an optimal and well-balanced QoS with seamless handover [8] and minimal switching cost. Section II describes the various scenarios involving DoS attack on 4G network. In section III

an introduction to SI is given, which is the back bone of the cognitive framework. Section IV gives a brief description on overcoming DoS attacks using the cognitive intelligence framework by formulating a combinatorial cost function using 4G network parameters. Section V concludes with a review on the key features of our approach and future work.

II. DoS ATTACK ON 4G NETWORK

A DoS attack on a network is typically by illegitimate users to reduce the capacity of the network or disrupt communication. Similarly, when the 4G network is encountered by a DoS attack, it reduces both the functionality and the overall performance causing inconvenience to both user and service provider. Hence, detecting DoS attacks and defending the network by taking the necessary countermeasures helps maintain and improve the performance of the application.

4G is a heterogeneous network that consists of technology from GSM to UMTS to WLAN and WiMax [4]. Each modulation technique faces jamming issues that can be the most debilitating form of DoS attack in the physical layer. Jamming attacks block or jam communication between the users's ME to the base station (BS) and also to any intermediate node (IN) if multi-hops are used.

A jammer is a device, which can partially or entirely disrupt a node's signal, by adding a noise signal overpowering the signal [10]. Jammers can never re-produce a signal nor pretend as a receiver node. Jammer parameters such as signal strength, location and type influence the performance of the network and each jammer having a different effect on the user. Whereas, partial band jamming (PBJ) causes interference in orthogonal frequency division multiplexing (OFDM) as shown in Figure 1 by Park et al.

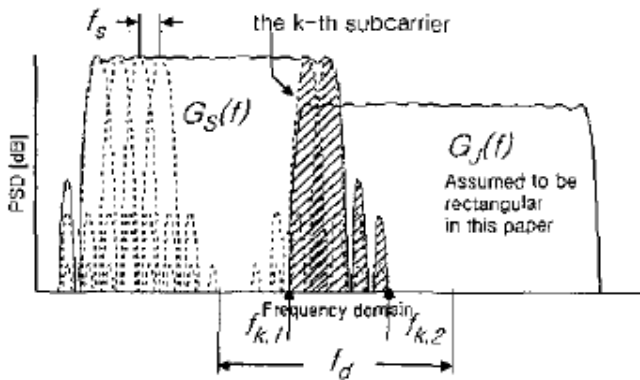


FIGURE 1: FREQUENCY SPECTRUM OF OFDM AND INTERFERENCE SIGNAL INSUFFICIENTLY SEPARATED [5]

DoS attacks in every layer based on the OSI network model can be classified as shown in Figure 2. Jammer and interference caused by the cell allocation takes places in the physical layer; whereas in the routing layer, collision attack and signaling attack causes the system to either go to shutdown. Sometimes the DoS attack can be both intentionally and un-intentioned. Either way, the percentage of lost

communication is more or less the same. In the transport layer, the possibility of flooding and authorization attack is high. In the application layer, authentication attacks are very common.

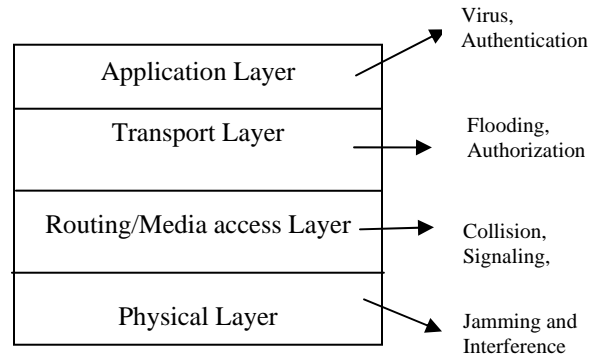


FIGURE 2: DENIAL OF SERVICE ATTACK ON 4G NETWORKS

The network is under threat if one or a combination of the DoS attacks occur; thus, cognitive algorithms can help by detecting and providing emergent solutions against such attacks. In the following section, the key features of cognitive intelligence are described.

III. COGNITIVE INTELLIGENCE

Evolutionary algorithms (EA) are formulated based on biological phenomena found in nature such as reproduction, mutation, recombination, natural selection and survival of the fittest. Two such evolutionary algorithms are the genetic algorithm and the ant system. The former is inspired by using simple genetic evolution of a living being, and the latter is inspired by studying the behavior of ants. The genetic algorithm (GA) was developed in the 1970's by John Holland at University of Michigan as a method to solve optimization problem. SI is an EA that uses artificial intelligence (AI) techniques.

SI demonstrates the collective behavior of social insects, namely the ants, bees, birds, slime mould, etc. In the early 90's, studies on optimization techniques using analogies based on swarm behavior of natural creatures has been conducted. Ant systems (AS) evolved from SI, and its key feature is the emergent behavior of the autonomous agents. Both GA and AS are specialized in their own ways for solving discrete continuous and hard combinatorial optimization problems. The algorithm chosen for any problem is primarily application dependent.

Gomez in [12] provides reasons for the success of Ant Colony Optimization (ACO) in comparison to GAs on the Travelling Salesman Problem (TSP) benchmark problem, a famous NP hard problem. The TSP solution space has a globally convex structure [14]. The presence of one dominant solution in GA results in a behavior like a single point search algorithm. GAs can easily produce a local solution rather than a global solution. Therefore when multiple solutions dominate a particular problem's population, the reduced diversity of GA

may result in an errored solution. Thus, GA falls short in situations like this where ACO, using positive correlation approaches where promising solution is located, may easily succeed.

The initial set of agents (ants) traverse in a random manner, and once they reach their destinations, they deposit pheromone on trails as a means of communicating indirectly with the other ants. The amount of pheromone left by the previous ant agents increases the probability that the same route is taken during the current iteration. Pheromone evaporation over time plays an important role in preventing suboptimal solutions from dominating in the beginning.

A Tabu-list serves as a memory tool listing the set of nodes that a single swarm agent has visited. The ant's goal is to visit nodes (ME or BS or IN) in the network depending on the number of hops assigned by the user. Thus traversing all the nodes and depleting all the energy at every node is avoided. In a given tour, a node is never re-visited. The pheromones on all the paths are updated at the end of a tour. The pheromone deposition, tabu-list, and energy monitoring help this novel swarm agent to obtain an optimal solution and adapt it as network degrades. A more detailed description of the cognitive intelligence algorithm can be found in our previous work [15, 16]

IV. PERFORMANCE OF 4G NETWORK USING COGNITIVE INTELLIGENCE

There are several different technologies used in 4G networks and DoS attacks have varied impact on each one. For example, Zigbee devices often run on batteries hence energy is an important aspect of this technology while something-of-death attack is crucial to WPA 802.1i [6]. Therefore, a cognitive framework is required, which responds intuitively to the changes in the environment while maintaining secure transmission and high throughput. Our approach can promise using cognitive intelligence for the following features in 4G network

1. Adaptive Modulation Scheme
2. Adaptive Error Correcting Scheme
3. Adaptive Energy Control Scheme
4. Adaptive Handover
5. Adaptive User interactions
6. Adaptive QoS features
7. Traffic Prioritization

There are some assumptions made in the 4G network such as, upon initialization of the network, the algorithm uses local information to perform cell dimensioning in a distributive manner unlike hierarchical or centralized approach used in traditional methods. Also, the BS is never under DoS attack whereas the IN and ME are prone to any open attacks.

Figure 3 illustrates the mobility management [2] performed by the cognitive framework by communicating with the BS at the region of interest which is denoted by two-way communication between the base station B, and dotted lines show the transition of the mobile user from the source in local region to destination in the outer region, where both have

different modulation and error correction schemes. The thick dark line forms a boundary between the two regions.

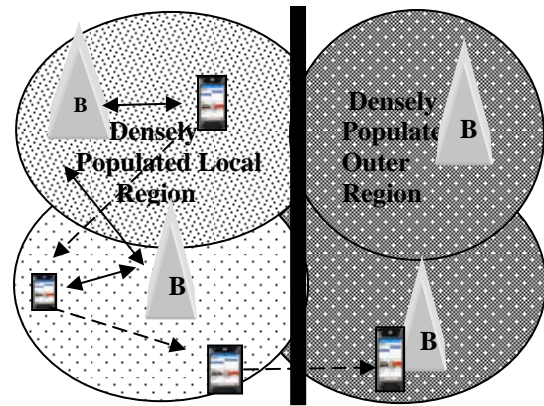
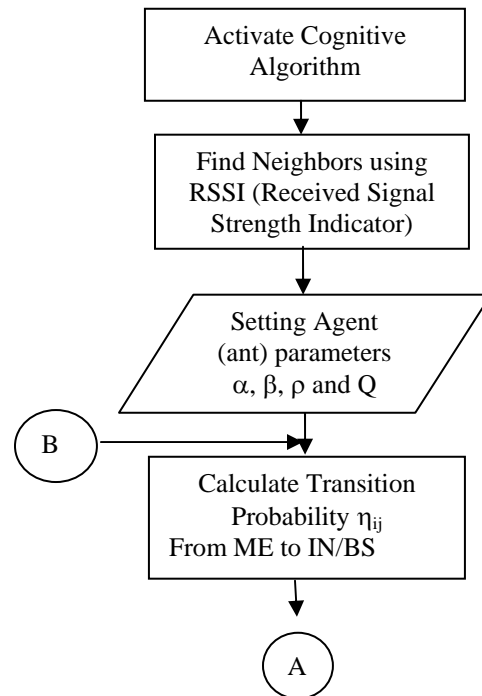


FIGURE 3: MOBILITY MANAGEMENT IN 4G USING COGNITIVE INTELLIGENCE

Upon detecting an event (mobile user) the agent communicates to BS and gathers information about its neighbors and finds the most optimal settings in order to provide high QoS and security depending on the resource availability of the mobile equipment. The optimal setting is formed based on the cost function, which weighs the performance parameters such as distance (D), number of hops (H), bit error rate (BER), packet delivery rate (PDR), signal strength (SS), energy (E), response time (RT), message prioritization and new call dropping probability (CPD). Depending upon the thresholds set for each parameter, the decision is made whether or not the call has successful call placements with high PDR and delay.



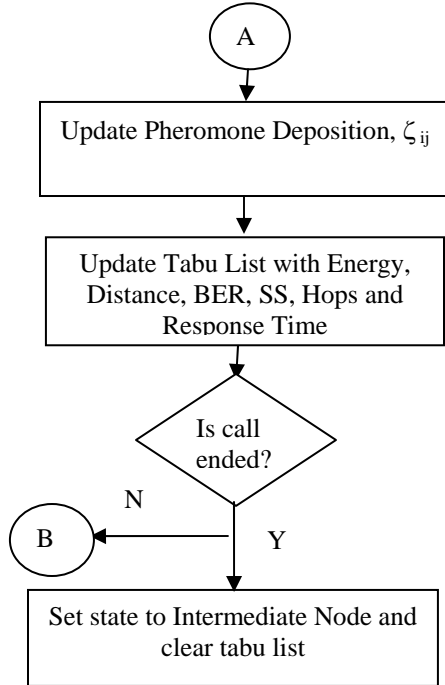


FIGURE 4: FLOWCHART OF COGNITIVE INTELLIGENCE

Figure 4 gives the step wise description of the cognitive approach to optimally select the channel that is best suited for communication. When a call is placed, the current resource availability of ME is detected. Depending on the value obtained the agents find the optimized route to reach the destination (BS/ME/IN). Since it's a mobile environment swarm agents continuously monitors the area of interest for any change in coverage area.

The swarm agents are spread randomly across the network. The agents communicate among each other using pheromone, and are initialized to 10 (arbitrary seed). The higher the value of pheromone in any particular path means it's the optimized path in terms of QoS and resource. The pheromone deposition is calculated based on the performance of the agent as

$$\zeta_{ij} = \rho(\zeta_{ij}(t-1)) + \frac{Q}{D_t \cdot E_t \cdot BER_t \cdot RT_t \cdot CPD_t} \quad (1)$$

where ij , means the transition from ME (source), i , to destination j (IN/BS), ρ is the memory and Q is an arbitrary parameter of the agent. Since the parameters used in the pheromone deposition depends on performance parameters, distance, energy, bit error rate, response time and call dropping probability. Degradation in any one of the parameter will reduce the pheromone deposition in that route. Therefore pheromone value on any particular path directly influences the transition probability of the agent, which exerts the movement of the agents.

$$\text{The transition probability } \eta_{ij} = \frac{(\psi_{ij})^\alpha \cdot (\xi_{ij})^\beta}{\sum_k (\psi_{ik})^\alpha \cdot (\xi_{ik})^\beta}$$

The performance parameter and pheromone deposition in the transition probability, ψ_{ij} , gives the movement of the agents between ME, BS and or IN.

$$\psi_{ij} = \frac{W_1 \cdot E_{ij} + W_2 \cdot D_{ij} + W_3 \cdot H_{ij} + W_4 \cdot RT_{ij} + W_5 \cdot CDP_{ij} + W_6 \cdot BER_{ij}}{\sum_k W_1 \cdot E_{ik} + W_2 \cdot D_{ik} + W_3 \cdot H_{ik} + W_4 \cdot RT_{ik} + W_5 \cdot CDP_{ik} + W_6 \cdot BER_{ik}}$$

The normalized value of performance parameters is used. In addition, weights W is applied to each of the parameters using goal lattice, [17], which is dependent on the application and QoS required by the user. The transition parameters, α and β , are used in balancing the message load across the network. One other important feature of the swarm agents is the tabu-list. This list, gives the route taken by the agents and the specific cost expended. The updated information of the tabu-list is shared among the agents, which helps agents attain time efficient and global optimized solutions. The trails formed by the ant agent are dependent on parameters obtained by a combination of both the physical and the MAC layers thus effectively avoiding DoS on these layers.

Cognitive Intelligence against Denial of Service Attack:

The performance parameters are included in the cost function of the cognitive algorithm and, also, the tabu list is continually updated. Thus, the neighbors are always aware of the current state of the mobile user. If the signal strength is weaker, or if the energy of the ME is strong but not responding to neighboring cells request, the user is considered jammed or having an interference attack. Similarly, if the PDR or the BER of the message has deteriorated, the system is experiencing a collision or signaling attack.

Likewise, the distance used in the agent's transition probability helps identify the IP based communication [11] of any impersonation. The updated tabu list helps in maintaining the previous movements of the user disabling any effort by the malicious user to impersonate. The weights can be increased to cover any number of performance parameters in the future improving flexibility, optimality, and overall efficiency of the network. During a real-time multimedia communication, the weights on the PDR and RT can grow to provide interactive services to the user.

Simulations were performed for Bluetooth and Zigbee enabled 4G network, where spread spectrum technology with gaussian frequency shift keying (GFSK), quadrature phase shift keying (QPSK) and binary phase shift keying was used (BPSK). The cognitive algorithm can also include biometric-face recognition for user authentication, thus achieving authorization to the data, application and hardware.

A hybrid of forward error correction code (FEC) using reed Solomon (RS) and automatic repeat on request (ARQ) were used as error correcting code. The results show the robustness of the cognitive algorithm against jammer attack.

TABLE I: COGNITIVE INTELLIGENCE AGAINST JAMMING ATTACK – USING BIOMETRIC AUTHENTICATION

# of jammed neighbors/ total neighbors	Average Energy	Average Packet Delivery %	Response Time	Jammer Type
3/25	15.2038	98.349	0.0020	Single Tone
9/25	30.4269	69.3568	0.0127	
16/25	50.0292	78.7423	0.0223	Jammer
3/25	0.2569	99.008	0.0050	Pulsed-Noise
9/25	7.4903	99.2105	0.0165	
16/25	31.920	78.9812	0.0288	Jammer

Table I demonstrates the robustness of cognitive intelligence against two types of jammer, namely, single tone jammer (ATJ) and pulsed-noise jammer (PNJ) [17]. These types of jammer attacks primarily focus on specific systems, where the STJ jams a narrowband channel and the PNJ jams a spread spectrum signal using an “On-Off” cyclic process. The simulation results show that even as the number of neighboring nodes that are under attack increases the performance of the network remains at 78%. When less than 10% of the neighboring cells are under attack, 98% QoS is achieved.

V. CONCLUSION AND FUTURE WORK

The main contribution in this paper is applying an adaptive cognitive algorithm to the 4G network to improve QoS and security of the network without using any complex methods. Since 4G is committed to providing heterogeneous service a cognitive intelligence is best suited as they can evolve and perform according to the user’s requirements rather than traditional deterministic methods. There are many complicated ways to solve DoS attacks that typically increase the response time and power of the system, using our approach DoS is easily captured with 96% detection rate while achieving an adaptive modulation, error correction, power control, handover, QoS, user interactions and traffic prioritization. The data collected by the tabu list can be further analyzed for anomalies using Bayesian network, which can be fed back to the agents to predict the DoS attack. Modulations such as OFDM, W-CDMA will be incorporated in our future work to evaluate real-time 4G network.

REFERENCES

[1] Zheng Y, He D, Yu W and Tang X, “ Trusted Computing-Based Security Architecture For 4G Mobile Networks”, Proc of 6th

International conf on Parallel and Distributed Computing, Applications and Technologies (PDCAT 05), 2005.

[2] Hussain S, Hamid Z and Khattak N.S., “ Mobility Management Challenges and Issues in 4G Hetrogenous Networks”, Proc of the 1st International Conf on Integrated Internet Ad hoc and Sensor Networks (InterSense 06), May 2006.

[3] Zheng Y, He D, Tang X and Wang H., “ AKA and Authorization Scheme for 4G Mobile Networks Based on Trusted Mobile Platform”, ICICIS 2005, 2005

[4] Roedig U and Sreenan C.J., “A Generic Hand-Over Framework for 4G Networks”, Information Technology & Telecommunications Conference (IT&T2006), Carlow, Ireland, October 2006.

[5] Park J, Kim D, Kang C and Hong D., “Effect of Partial Band Jamming on OFDM-Based WLAN in 802.11G”, ICASSP 2003.

[6] Egli P., “Susceptibility of Wireless Devices to Denial of Service attacks”, White paper, Netmodule AG, Niederwangen, Switzerland

[7] Lee P.C.P, Bu T and Woo T., “On the Detection of Signaling DoS attacks on 3G Wireless Networks”, Proceeding of IEE INFOCOM, Anchorage, Alaska, May 2007.

[8] Binanchi G, Tinnirello and Scalia L., “Handover across Heterogeneous Wireless System: a Platform-Independent Control Logic Design”, WPMC 2003, Ottobre, Yokosuka.

[9] Kennedy J, Shi Y and Eberhart R.C., “Swarm Intelligence”, Morgan Kaufmann Publishers, San Francisco, 2001.

[10] Muraleedharan R and Osadciw L.A., “Security: Cross Layer Protocols in Wireless Sensor Networks”, IEEE INFOCOM, Student workshop, Barcelona, Spain, April 2006.

[11] Prasad A and Schoo P., “IP Security for Beyond 3G Towards 4G”, In Proceeding of WWRF, Eindhoven, Netherlands, Dec 3-4 2002.

[12] Osvaldo G and Benjamín B., “Reasons of ACO’s Success in TSP”, In Ant Colony, Optimization and Swarm Intelligence, vol 3172 of LNCS, Brussels, September 2004. Springer-Verlag

[13] E. Bonabeau, M. Dorigo, and G. Théraulaz, “ Swarm intelligence: from natural to artificial systems”, Oxford University Press, 1999

[14] T. C. Hu, Victor Klee, and David Larmann., “Optimization of globally convex functions “, SIAM Journal on Control and Optimization, 27(5):1026–1047, September 1989.

[15] Muraleedharan R and Osadciw L.A., “A Predictive Sensor Network Using Ant Systems “, SPIE Defence and Security, Orlando, Apr 12-17, 2004.

[16] Muraleedharan R, Yanjun Y and Osadciw L.A., “ Detecting Sybil Attack in Image Sensor Network Using Cognitive Intelligence “, In Proc of ACM Workshop on Sensor Actor Network, Montreal, Canada, Sept 2007.

[17] Muraleedharan R and Osadciw L.A., “ Jamming attack Detection and Countermeasures in Wireless Sensor Network Using Ant System”, SPIE Defence and Security, Orlando, Apr 12-17, 2006