Volume 2, Issue 8, August 2012 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

Secure Communications over Wireless Broadcast Networks Using Shortest Seek First Algorithm

[1]MD SIRAJUL HUQUE, [2] P. ANJANEYULU, [3] A. TIRUPATHAIAH
Dept of Information Technology, JNTUK
Hyderabad, India

Abstract: ***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 kilometers for deep-space radio communications. In this paper wireless broadcast network model(WBN) with secrecy constraints is investigated, in which a source node broadcasts confidential message flows to user nodes, with each message intended to be decoded accurately by one user and to be kept secret from all other users. In the existing system we developed, and implemented a compromised router detection protocol (DP) that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses (CPL) that will occur. Each and every packet is encrypted so that to prevent the data from eavesdropping. So the data is much secured. Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions, still existing system is a good experiment but it will take more time while it's in the process. So to overcome this along with the queue method we proposing shortest seek first algorithm (SSFA) for the better results to overcome the drawback of lacking time.***

Key words: WBN, DP, CPL, SSFA.

1. INTRODUCTION

Wireless operations permit services, such as long range communications, that are impossible or impractical to implement with the use of wires. The term is commonly used in the telecommunications industry to refer to telecommunications systems (e.g. radio transmitters and receivers, remote controls, computer networks, network terminals, etc.) which use some form of energy (e.g. radio frequency (RF),acoustic energy, etc.) to transfer information without the use of wires.[1] Information is transferred in this manner over both short and long distances. Wireless networking (i.e. the various types of unlicensed 2.4 GHz WiFi devices) is used to meet many needs. Perhaps the most common use is to connect laptop users who travel from location to location.[1] Another common use is for mobile networks that connect via satellite. A wireless transmission method is a logical choice to network a LAN segment that must frequently change locations. The following situations justify the use of wireless technology:

- To span a distance beyond the capabilities of typical cabling,
- To provide a backup communications link in case of normal network failure,
- To link portable or temporary workstations,
- To overcome situations where normal cabling is difficult or financially impractical, or
- To remotely connect mobile users or networks.[2]

1.1 MODES: Wireless communications can be via:

- radio frequency communication,
- microwave communication, for example long-range line-of-sight via highly directional antennas, or short-range communication,
- Infrared (IR) short-range communication, for example from consumer IR devices such as remote controls or via Infrared Data Association (IrDA).

Applications may involve communication, point, broadcasting, cellular networks and other wireless networks.

1.2 CORDLESS: The term "wireless" should not be confused with the term "cordless", which is generally used to refer to powered electrical or electronic devices that are able to operate from a portable power source (e.g. a battery pack) without any cable or cord to limit the mobility of the cordless device through a connection to the mains power supply.

Some cordless devices, such as cordless telephones, are also wireless in the sense that information is transferred from the cordless telephone to the telephone's base unit via some type of wireless communications link. This has caused some disparity in the usage of the term "cordless", for example in Digital Enhanced Cordless Telecommunications.[3]

1.3 APPLICATIONS OF WIRELESS TECHNOLOGY

Mobile telephones
One of the best-known examples of wireless technology is the mobile phone, also known as a cellular phone, with more than 4.6 billion mobile cellular subscriptions worldwide as of the end of 2010. These wireless phones use radio waves to enable their users to make phone calls from many locations worldwide. They can be used within range of the mobile telephone site used to house the equipment required to transmit and receive the radio signals from these instruments.

Wireless data communications
Wireless data communications are an essential component of mobile computing. The various available technologies differ in local availability, coverage range and performance, and in some circumstances, users must be able to employ multiple connection types and switch between them. To simplify the experience for the user, connection manager software can be used, or a mobile VPN deployed to handle the multiple connections as a secure, single virtual network.

Supporting technologies include:

Wi-Fi is a wireless local area network that enables portable computing devices to connect easily to the Internet. Standardized as IEEE 802.11 a,b,g,n, Wi-Fi approaches speeds of some types of wired Ethernet. Wi-Fi has become the de facto standard for access in private homes, within offices, and at public hotspots.[14] Some businesses charge customers a monthly fee for service, while others have begun offering it for free in an effort to increase the sales of their goods.

Cellular data service offers coverage within a range of 10-15 miles from the nearest cell site. Speeds have increased as technologies have evolved, from earlier technologies such as GSM, CDMA and GPRS, to 3G networks such as W-CDMA, EDGE or CDMA2000.

Mobile Satellite Communications may be used where other wireless connections are unavailable, such as in largely rural areas[18] or remote locations. Satellite communications are especially important for transportation, aviation, maritime and military use.

Wireless energy transfer
Wireless energy transfer is a process whereby electrical energy is transmitted from a power source to an electrical load that does not have a built-in power source, without the use of interconnecting wires.

Computer interface devices
Answering the call of customers frustrated with cord clutter, many manufactures of computer peripherals turned to wireless technology to satisfy their consumer base. Originally these units used bulky, highly limited transceivers to mediate between a computer and a keyboard and mouse, however more recent generations have used small, high quality devices, some even incorporating Bluetooth. These systems have become so ubiquitous that some users have begun complaining about a lack of wired peripherals. Wireless devices tend to have a slightly slower response time than their wired counterparts, however the gap is decreasing. Concerns about the security of wireless keyboards arose at the end of 2007, when it was revealed that Microsoft's implementation of encryption in some of its 27 MHz models was highly insecure. [3][4]

1.4 TYPES OF WIRELESS NETWORKS

Wireless PAN Wireless personal area networks (WPANs) interconnect devices within a relatively small area, that is generally within a person's reach. For example, both Bluetooth radio and invisible infrared light provides a WPAN for interconnecting a headset to a laptop. ZigBee also supports WPAN applications. Wi-Fi PANs are becoming commonplace (2010) as equipment designers start to integrate Wi-Fi into a variety of consumer electronic devices. Intel "My WiFi" and Windows 7 "virtual Wi-Fi" capabilities have made Wi-Fi PANs simpler and easier to set up and configure.

Wireless LAN
Main article: Wireless LAN: A wireless local area network (WLAN) links two or more devices over a short distance using a wireless distribution method, usually providing a connection through an access point for Internet access. The use of spread-spectrum or OFDM technologies may allow users to move around within a local coverage area, and still remain connected to the network.

Products using the IEEE 802.11 WLAN standards are marketed under the Wi-Fi brand name. Fixed wireless technology implements point-to-point links between computers or networks at two distant locations, often using dedicated microwave or modulated laser light beams over line of sight paths. It is often used in cities to connect networks in two or more buildings without installing a wired link.

Wireless mesh network

Main article: wireless mesh network : A wireless mesh network is a wireless network made up of radio nodes organized in a mesh topology. Each node forwards messages on behalf of the other nodes. Mesh networks can "self heal", automatically re-routing around a node that has lost power.

Wireless MAN

Wireless metropolitan area networks are a type of wireless network that connects several wireless LANs.

- WiMAX is a type of Wireless MAN and is described by the IEEE 802.16 standard.

Wireless WAN

Wireless wide area networks are wireless networks that typically cover large areas, such as between neighboring towns and cities, or city and suburb. These networks can be used to connect branch offices of business or as a public internet access system. The wireless connections between access points are usually point to point microwave links using parabolic dishes on the 2.4 GHz band, rather than unidirectional antennas used with smaller networks. A typical system contains base station gateways, access points and wireless bridging relays. Other configurations are mesh systems where each access point acts as a relay also. When combined with renewable energy systems such as photo-voltaic solar panels or wind systems they can be stand alone systems.[5][4]

Cellular network Main article: cellular network

FIG 1: Top of a cellular radio tower

A cellular network or mobile network is a radio network distributed over land areas called cells, each served by at least one fixed-location transceiver, known as a cell site or base station. In a cellular network, each cell characteristically uses a different set of radio frequencies from all their immediate neighboring cells to avoid any interference.

When joined together these cells provide radio coverage over a wide geographic area. This enables a large number of portable transceivers (e.g., mobile phones, pagers, etc.) to communicate with each other and with fixed transceivers and telephones anywhere in the network, via base stations, even if some of the transceivers are moving through more than one cell during transmission.[6]

Although originally intended for cell phones, with the development of smart phones, cellular telephone networks routinely carry data in addition to telephone conversations:

- Global System for Mobile Communications (GSM): The GSM network is divided into three major systems: the switching system, the base station system, and the operation and support system. The cell phone connects to the base system station which then connects to the operation and support station; it then connects to the switching station where the call is transferred to where it needs to go. GSM is the most common standard and is used for a majority of cell phones.
- Personal Communications Service (PCS): PCS is a radio band that can be used by mobile phones in North America and South Asia. Sprint happened to be the first service to set up a PCS.
- D-AMPS: Digital Advanced Mobile Phone Service, an upgraded version of AMPS, is being phased out due to advancement in technology. The newer GSM networks are replacing the older system.[7]

1.5 USES

Some examples of usage include cellular phones which are part of everyday wireless networks, allowing easy personal communications. Another example, Inter-continental network systems, use radio satellites to communicate across the world. Emergency services such as the police utilize wireless networks to communicate effectively as well. Individuals and businesses use wireless networks to send and share data rapidly, whether it be in a small office building or across the world.

General "Now, the industry accepts a handful of different wireless technologies. Each wireless technology is defined by a standard that describes unique functions at both the Physical and the Data Link layers of the OSI Model. These standards differ in their specified signaling methods, geographic ranges, and frequency usages, among other things. Such differences can make certain technologies better suited to home networks and others better suited to network larger organizations."

Performance Each standard varies in geographical range, thus making one standard more ideal than the next depending on what it is one is trying to accomplish with a wireless network.[8] The performance of wireless networks satisfies a variety of applications such as voice and video. The use of this technology also gives room for future expansions. As wireless networking has become commonplace , sophistication increased through configuration of network hardware and software.

Space Space is another characteristic of wireless networking. Wireless networks offer many advantages when it comes to difficult-to-wire areas trying to communicate such as across a street or river, a warehouse on the other side of the premise or buildings that are physically separated but operate as one.[9] Wireless networks allow for users to designate a certain space which the network will be able to communicate with other devices through that network. Space is also created in homes as a result of eliminating clutters of wiring. This techonology allows for an alternative to installing physical network mediums such as TPs, coaxes, or fiber-optics, which can also be expensive.

Home For homeowners, wireless technology is an effective option as compared to ethernet for sharing printers, scanners, and high speed internet connections. WLANs help save from the cost of installation of cable mediums, save time from physical installation, and also creates mobility for devices connected to the network.[10] Wireless networks are simple and require as few as one single wireless access point connected directly to the Internet via a router**.**

Environmental concerns Starting around 2009, there have been increased concerns about the safety of wireless communications, despite little evidence of health risks so far. The president of Lakehead University refused to agree to installation of a wireless network citing a California Public Utilities Commission study which said that the possible risk of tumors and other diseases due to exposure to electromagnetic fields (EMFs) needs to be further investigated.
Wireless access points are also often close to humans, but the drop off in power over distance is fast, following the inverse-square law. The HPA's position is that "...radio frequency (RF) exposures from WiFi are likely to be lower than those from mobile phones." It also saw "...no reason why schools and others should not use WiFi equipment." In October 2007, the HPA launched a new "systematic" study into the effects of WiFi networks on behalf of the UK government, in order to calm fears that had appeared in the media in a recent period up to that time". Dr Michael Clark, of the HPA, says published research on mobile phones and masts does not add up to an indictment of WiFi. [8]

1. Related Literature work:

Wireless broadcast networks constitute one class of basic and important wireless networks, in which a source node simultaneously transmits a number of information communications make use of the open nature of the wireless medium, which presents a great challenge to achieve secure communication for individual users. This is because information for all users is contained in one transmitted signal, and hence information destined for one user may be obtained by
no intended users unless special coding is used. Physical layer security, which uses randomness of a physical communication channel to provide security for messages transmitted through
the channel, opens a promising new direction toward solving wireless networking security problems. This approach was pioneered by Wyner in [1] and by Csiszár and Körner in [2],
and more recently has been extensively explored in the literature (see [3] for a review of recent advances in physical layer security).

Physical layer security adopts a precise quantitative measure of security level, i.e., the *equivocation rate* defined by Shannon [4], which equals the entropy rate of the source message conditioned on the channel output at the eavesdropper.

This measure of the secrecy level allows security to be considered under the general Shannon framework of information theory [5], and hence provides an analytical basis with which to characterize the fundamental limits on communication rates given the security level constraints. This measure of security level also makes a unified security design across networking layers possible. The goal of such a design is to maximize network utility (i.e., to maximize overall users' satisfaction of the service rate in a certain fair manner among users) under security, reliability, and stability constraints. This motivates a joint design of rate control at the transport layer, rate scheduling at the medium access control layer, and power control and secure coding at the physical layer.

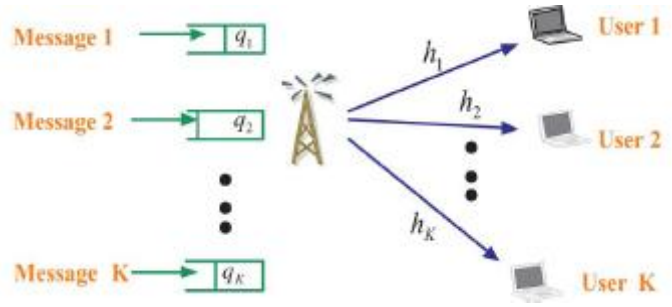

Fig 2: Fading broadcast Network.

We assume that the channel from the source to the users is a fading broadcast channel, in which the channel outputs at each user are corrupted by a multiplicative fading gain process in addition to an additive white Gaussian noise process. We assume that the channel state information (channel gain realization) is known to the source node and to the corresponding receiver. This assumption is justified in the broadcast scenario considered here, because all users receive information from the source node and hence it is reasonable for them to feed their channel states back to the source node to obtain better service rates from this node. There are two time scales (see Fig. 3): one is the symbol time level, at which the channel state varies across symbol times, and the other is the packet time level, which spans a large number of symbol times during which the channel state behaves erotically.[9]

To achieve reliable and secure communication for users, we adopt the physical layer security approach [1], [2] to employ a stochastic encoder at the source node. The source node allocates its power not only among message flows (i.e., among users) but also dynamically according to the channel state information to improve secrecy communication rates. Hence the source power control operates over the symbol time scale, and determines the service rate allocation among users at the packet time level. At the packet time level, to maintain the stability of all queues, the
source node implements a rate schedule scheme that adapts its service rate allocation dynamically among users based on the queue lengths. Furthermore, rate control is performed also at the packet time level to maximize the network utility function. Our goal is to study how to jointly design rate control and rate scheduling at the packet time scale and power control and secure coding at the symbol time scale to achieve network utility maximization under reliability, security and stability constraints.

For the collaborative eaves dropping model, we first obtain the secrecy capacity region, within which each rate vector can be achieved by a time-division scheme, i.e., at each channel state, the source transmits only to the user whose channel gain is better than the sum of the channel gains of all other users. It is clear that this user must have the best channel gain at this state. The power control among the channel states thus determines the rate allocation among users, i.e., rate allocation among components of a rate vector. We further show that all arrival rate vectors contained in this region can be stabilized by a throughput optimal queue-length-based scheduling scheme at the packet time level, where queue length determines the service rate allocation among users, and hence determines the corresponding power control to achieve this service rate vector at the symbol time level.[10] Finally, we obtain a distributed rate control policy that Maximizes the overall network utility maximization given that reliability, secrecy, and stability are achieved. This maximization is achieved by joint design of rate control, rate scheduling, power control, and secure coding.

For the non collaborative eavesdropping model, we study a time-division scheme, in which the source transmits to one user in each channel state. The secrecy rate region based on this scheme is derived. Although the time-division scheme is suboptimal, it is simple and important from a practical point of view. We also provide and discuss improved secure coding schemes based on non-time-division schemes. Based on a simple achievable secrecy rate region, a queue-length-based rate scheduling algorithm is derived that stabilizes the arrival rate vectors contained in this rate region. We also obtain the distributed rate control policy that achieves the overall network utility maximization.[11]

2. MODEL

Our proposed model is shortest seek first algorithm it scans the request queue for the request that is nearest the head and serves that request first.

- This algorithm minimizes the total seeking that the head must perform
- This algorithm can allow requests to starve. If new requests keep coming in that are near the current position of the head at a sufficient rate, the disk head will never move near enough to other requests to service them.

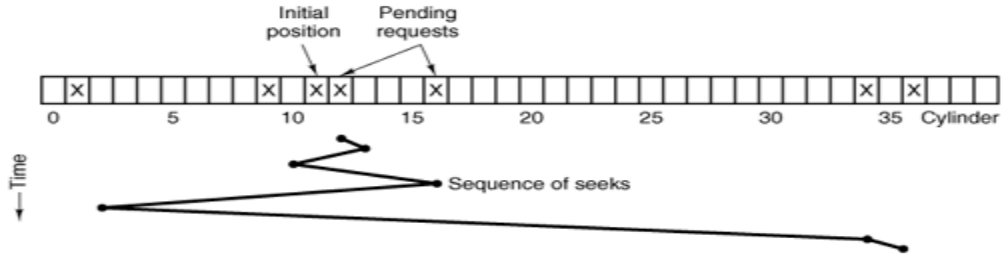

Fig 4:Shortest seek first scheduling algorithm.

This is a direct improvement upon a first-come first-served (FIFO) algorithm. The drive maintains an incoming buffer of requests, and tied with each request is a cylinder number of the request. Lower cylinder numbers indicate that the cylinder is closer to the spindle, while higher numbers indicate the cylinder is farther away. The shortest seek first algorithm determines which request is closest to the current position of the head, and then services that request next.

We consider the -user fading broadcast network (see Fig. 1), in which a source node transmits confidential messages to user nodes. Each message is intended for one user and needs to be kept secret from all other nodes. Hence, with regard to one message, all users other than its intended receiver are considered to be eavesdroppers. We assume that the channel from the source node to the users is a fading broadcast channel, in which the channel outputs at each user are corrupted by a multiplicative fading gain process in addition to an additive white Gaussian noise process.[12]
The channel input–output relationship is given by

$$y_{in}=h_{in} .\ x_n+ w_{in} \text{ for } 1\leq I \leq k \ldots\ldots..(1).$$

Where denotes the th user, and denotes the n th symbol time instant. At the symbol time instant, is the channel input from the source, is the channel output at user , is the source-to-user channel gain coefficient, and is the noise term at user . We define, and assume is a stationary and periodic vector proper complex random process. We assume that the channel state information (i.e., the realization of) is known at both the source node and the corresponding receivers. Here, the fading coefficients
across users are not necessarily independent, and nor are they necessarily identically distributed. It will be as long as the channel state information is known, only the marginal channel distributions to individual users affect the performance of the network. The noise processes for are independent identically distributed (i.i.d.) proper complex Gaussian processes with zero means and unit variances. The input sequence {Xn} is subject to the average power constraint, i.e.,

$$1/N.\ \frac{1}{N} = \sum_{N=1}^{n} E(X2n\ ) \leq P \ldots\ldots\ldots\ldots(2).$$

The secrecy capacity region is defined to be the set that includes all achievable rate vectors such that perfect secrecy can be achieved. Since the source node has access to the channel state information, the source can dynamically change its transmission power as the channel state varies at the symbol time level. Each rate vector in the secrecy capacity region is a service rate allocation among users and is achieved by a corresponding power control policy at the source node.

We assume that the source node maintains one queue for each message flow if it is not served immediately. We first consider the case in which the arrivals of the message flows are on the packet time scale, and are assumed to be random and independent of each other. We use to denote an arrival rate vector at packet time slot, with each component representing the arrival rate of one queue at packet time slot. The system is stochastically stable if no queue builds to infinity. We use the vector to denote the queue length vector at packet time slot, with each component denoting the queue length for the th queue. We note that each packet time slot contains a large number of symbol time slots, during which the channel state changes in a stationary and ergodic manner. For each packet time slot, the rate scheduling at the source node is accomplished by choosing a secrecy rate vector as a service rate vector, which is achieved by a corresponding power control policy at the symbol time level. The stability region is defined to include all arrival rate vectors that can be stabilized by a rate scheduling algorithm.[13]

In the second case, we assume that associated with each user, a standard -fair utility function is given by

$$U_i(x_i) = \kappa_i \frac{x_i^{1-\alpha_i}}{1-\alpha_i} \quad \ldots\ldots\ldots\ldots (3).$$

where denotes the rate at which the source node generates the messages for user . The objective is to control arrival rate vectors for users properly so that the following network utility function is maximized, i.e.,

$$\max_{\underline{x} \in C_s} \sum_i U_i(x_i) \quad \text{.....(4).}$$

3. ANALYSIS

The shortest seek first algorithm has the direct benefit of simplicity and is clearly advantageous in comparison to the FIFO method, in that overall arm movement is reduced, resulting in lower average response time. However, since the buffer is always getting new requests, these can skew the service time of requests that may be farthest away from the disk head's current location, if the new requests are all close to the current location; in fact, starvation may result, with the faraway requests never being able to make progress. The elevator algorithm is one way of reducing arm movement/response time, and ensuring consistent servicing of requests.[12]

The elevator algorithm (also SCAN) is a disk scheduling algorithm to determine the motion of the disk's arm and head in servicing read and write requests. This algorithm is named after the behavior of a building elevator, where the elevator continues to travel in its current direction (up or down) until empty, stopping only to let individuals off or to pick up new individuals heading in the same direction. From an implementation perspective, the drive maintains a buffer of pending read/write requests, along with the associated cylinder number of the request. Lower cylinder numbers indicate that the cylinder is closest to the spindle, and higher numbers indicate the cylinder is further away. When a new request arrives while the drive is idle, the initial arm/head movement will be in the direction of the cylinder where the data is stored, either *in* or *out*. As additional requests arrive, requests are serviced only in the current direction of arm movement until the arm reaches the edge of the disk. When this happens, the direction of the arm reverses, and the requests that were remaining in the opposite direction are serviced, and so on.[13][14]

VARIATIONS: One variation of this method ensures all requests are serviced in only one direction, that is, once the head has arrived at the outer edge of the disk, it returns to the beginning and services the new requests in this one direction only (or vice versa). This is known as the "Circular Elevator Algorithm" or C-SCAN. This results in more equal performance for all head positions, as the expected distance from the head is always half the maximum distance, unlike in the standard elevator algorithm where cylinders in the middle will be serviced as much as twice as often as the innermost or outermost cylinders.

Other variations include

- **FSCAN**: FScan is a disk scheduling algorithm to determine the motion of the disk's arm and head in servicing read and write requests. It uses two subqueues. During the scan, all of the requests are in the first queue and all new requests are put into the second queue. Thus, service of new requests is deferred until all of the old requests have been processed. When the scan ends, the arm is taken to the first queue entries and is started all over again.

Analysis: FSCAN along with N-Step-SCAN prevents "arm stickiness" unlike SSTF, SCAN, and C-SCAN. Arm stickiness in those other algorithms occurs when a stream of requests for the same track causes the disk arm to stop progressing at that track, preferring to satisfy the no-seek requests for the track it is on. Because FSCAN separates requests into two queues, with new requests going into a waiting queue, the arm continues its sweep to the outer track and is therefore not "sticky." There is an obvious trade-off in that the requests in the waiting queue must wait longer to be fulfilled, but in exchange FSCAN is more fair to all requests.

- LOOK (and C-LOOK): LOOK is a disk scheduling algorithm used to determine the order in which new disk read and write requests are processed. LOOK is similar to SCAN in that the heads sweep across the disk surface in both directions performing reads and writes. However, unlike SCAN, which visits the innermost and outermost cylinders each sweep, LOOK will change directions when it has reached the last request in the current direction.[15]

Variant: One variant of LOOK is C-LOOK, which fulfills requests in one direction only. That is, C-LOOK starts at the innermost cylinder requested and moves outward fulfilling requests until it reaches the last request. Then it moves directly back to the innermost request and starts fulfilling requests moving outward again.

Performance: LOOK has slightly better average seek times than SCAN. C-LOOK has a slightly lower variance in seek time than LOOK since the worst case seek time is nearly cut in half.

- **N-Step-SCAN:** (also referred to as N-Step LOOK) is a disk scheduling algorithm to determine the motion of the disk's arm and head in servicing read and write requests. It segments the request queue into subqueues of length N. Breaking the queue into segments of N requests makes service guarantees possible. Subsequent requests entering the request queue won't get pushed into N sized subqueues which are already full by the elevator algorithm. As such, starvation is eliminated and guarantees of service within N requests is possible.

Analysis: N-Step-SCAN along with FSCAN prevents "arm stickiness" unlike SSTF, SCAN, and C-SCAN.

A. *Secrecy Capacity Region:* In this section, we consider the collaborative eavesdropping model, in which for a given message, all users (eavesdroppers) other than the intended destination can exchange their outputs to try to decode a given message. Since the eavesdroppers can exchange their outputs, they can be viewed as a super-eavesdropper that has receive antennas with each antenna receiving the outputs of one eavesdropper. Hence, the channel is equivalent to the wiretap channel [1] with the eavesdropper having multiple antennas, whose secrecy capacity can be obtained from that for the multiple-input multiple-output (MIMO) wiretap channel. It is then clear that for each channel state, only a user whose channel gain is larger than the sum of the channel gains of all other users (eavesdroppers) can receive its message with perfect Secrecy. Note that such a user may not exist. It is clear that this user must have the best channel state among all users. This suggests a time-division scheme with the source transmitting to at most one user in each channel state .For a given channel state , let denote the source power allocation for state . We use to denote the set that includes all power allocation functions (i.e., power control policies) that satisfy the power constraints, i.e.,

$$\mathcal{P} = \{p(\underline{h}) : E[p(\underline{h})] \leq P\}. \quad \text{.....(5)}$$

Now let be the set of all channel states for which the channel gain of user is larger than the sum of the channel gains of all other users, i.e.,

$$\mathcal{A}_i = \left\{ \underline{h} : |h_i|^2 \geq \sum_{j \neq i, 1 \leq j \leq K} |h_j|^2 \right\}. \quad \text{.....(6)}$$

The following theorem states that a time-division scheme is optimal to achieve the secrecy capacity region.

$$\mathcal{C}_s = \bigcup_{p(\underline{h}) \in \mathcal{P}} \left\{ \begin{array}{l} (R_1, \ldots, R_K): \\ R_i \leq E_{\underline{h} \in A_i} \left[\log(1 + p(\underline{h})|h_i|^2) \right. \\ \qquad \left. - \log\left(1 + p(\underline{h}) \sum_{j \neq i, 1 \leq j \leq K} |h_j|^2\right) \right] \\ \text{for } 1 \leq i \leq K \end{array} \right\} \quad \text{.....(7)}$$

Theorem 1: For the collaborative eavesdropping model, the secrecy capacity region of the fading broadcast network is given by where the random vector h= (h1,…….hk) has the same distribution as the marginal distribution of the random process h= ∞ at one symbol time instant.

B. Stability and Utility Maximization

The secrecy capacity region given in Theorem 1 includes all achievable secrecy rate vectors with each component representing the service rate for one user. It still remains to determine a rate scheduling algorithm to choose a service rate vector at each packet time slot to stabilize all queues and correspondingly to determine a power control policy over the symbol time slots to achieve this service rate vector. The rate scheduling algorithm and the power allocation policy are given in the following two theorems, respectively.

Theorem 2: For the collaborative eavesdropping model, the information flows (i.e., the queues) are stable only if the arrival rate vector is in the secrecy capacity region given, i.e., . Furthermore, given any arrival rate vector that satisfies (where denotes a –dimensional vector with all components equal to), the system is stochastically
stable under the following queue-length-based algorithm:

for any given queue length vector q[t] , the secrecy rate vector r[t] is chosen to be a solution to the following optimization problem:

$$\max_{(R_1,\ldots,R_K)\in\mathcal{C}_s} q_1[t]R_1 + \cdots + q_K[t]R_K. \quad \text{…….(8).}$$

The channel states in this set may not necessarily satisfy the condition that user has the best channel state among all users. The channel corresponding to these states can be viewed as parallel channels to every user with each subchannel corresponding to one state realization . Since during these states, the source node transmits information only to user , this channel is a parallel compound wiretap channel with user being the legitimate receiver and other users being eavesdroppers, and both the legitimate user and eavesdroppers having parallel Gaussian channels. For the compound parallel wiretap channel, an optimal secure coding scheme was proposed in to code across all parallel channels. Applying this scheme, an achievable rate for user can be obtained and is given by

$$R_i = \min_{j\neq i} E_{\underline{h}:A(\underline{h})=i}\left[\log\left(1+p(\underline{h})|h_i|^2\right) - \log\left(1+p(\underline{h})|h_j|^2\right)\right]^+ \quad \text{.....[9]}$$

Where [.] $^+$equals its argument if it is positive and equals zero otherwise. It is clear that the total power allocated for transmitting to user is given by

$$E_{\underline{h}:A(\underline{h})=i}[p(\underline{h})]. \quad \text{……(10).}$$

Similar to the above steps, we can obtain the achievable secrecy rates for other users, and hence these rates constitute a rate vector achieved for a given power control scheme p[h] and a channel allocation scheme A[h] . An achievable secrecy rate region for the broadcast channel includes achievable secrecy rates obtained for any power control scheme and any possible state allocation
scheme, which is given below.

Theorem 3: For the noncollaborative eavesdropping model, an achievable secrecy rate region for the fading broadcast channel is given by

$$\mathcal{R}_s = \bigcup_{p(\underline{h})\in\mathcal{P}, A(\underline{h})\in\mathcal{A}} \left\{ \begin{array}{l} (R_1,\ldots,R_K): \\ R_i = \min_{j\neq i} E_{\underline{h}:D(\underline{h})=i}\left[\log\left(1+p(\underline{h})|h_i|^2\right) - \log\left(1+p(\underline{h})|h_j|^2\right)\right]^+ \\ \text{for } 1\leq i\leq K \end{array} \right\} \quad \text{…… (11)}$$

Where the random vector has the same distribution as the marginal distribution of the random process at one symbol time instant. We further consider a simple state allocation function, in
which the source node transmits to user if user 's channel is the best among users. We define the set to include all such channel states, i.e.,

$$\mathcal{A}_i = \left\{\underline{h} : |h_i|^2 \geq |h_j|^2 \ \forall\, j\neq i, 1\leq j\leq K\right\} \quad \text{…….(12)}$$

Then we have the state allocation function if for. Based on this state allocation function, we have the following corollary. Corollary 1: For the non collaborative eavesdropping model, an achievable secrecy rate region for the fading broadcast channel is given by

$$\mathcal{R}_s^1 = \bigcup_{p(\underline{h})\in\mathcal{P}} \left\{ \begin{array}{l} (R_1,\ldots,R_K): \\ R_i \le \min\limits_{j\neq i, 1\le j\le K} E_{\underline{h}\in A_i}\Big[\log\left(1+p(\underline{h})|h_i|^2\right) \\ \qquad\qquad - \log\left(1+p(\underline{h})|h_j|^2\right)\Big] \\ \text{for } 1\le i\le K \end{array} \right\} \quad \ldots\ldots\ldots\ldots(13)$$

where the random vector has the same distribution as the marginal distribution of the random process at one symbol time instant.

Proof: For each channel state, the source transmits only to the user with the best channel state, and hence the channel is the wiretap channel with multiple eavesdroppers. The achievable
Secrecy rate follows directly from the proof.

We note that similar to the collaborative eavesdropping model, each rate in (16) decreases as the number of users increases; because the number of rate terms that the "min" is taken over increases. We also note that the gap between the regions given in (14) and (9) suggests the impact of eavesdropper collaboration on the secrecy rate region. Two major differences determine the gap between the two regions. First of all, for the collaborative avesdroppingmodel, collaboration among eavesdroppers is reflected by the fact that a rate determined by the sum of the channel gains of the eavesdroppers is subtracted from the rate to the legitimate user in (9). For the no collaborative eavesdropping model, a rate determined by the channel gain of each individual user is subtracted from the rate to the legitimate user. Second, for the collaborative model, a positive secrecy rate is achievable for a channel state only if one user has its channel gain larger than the sum of the channel gains of all of the other users. This condition may not be satisfied by all channel states. Hence, there may be some channel states at which no user can receive a positive secrecy rate. However, for the no collaborative model, the condition for a user to achieve a positive secrecy rate is that this user's channel gain is larger than that of all other users. This condition is less stringent, and each channel state can satisfy this Condition for a certain user and hence contributes to this user's secrecy rate. Due to both of the above reasons, the secrecy rate region for the no collaborative eavesdropping model is larger Than that of the collaborative eavesdropping model. This justification suggests the following remark. Remark 4: The regions given in (14) and (16) are larger than the region given in (9). This is because the eavesdroppers are less powerful in the no collaborative eavesdropping model than in the collaborative eavesdropping model. Further improved secrecy rate regions can be derived if the source node is not restricted to time-division schemes and transmits multiple information flows at a time. In this case, the state allocation function represents a set of user indices to which the source node transmits at the channel state , and becomes more involved. The source node can apply stochastic superposition coding [45] to transmit multiple information flows simultaneously at one channel state. For each user, secure coding is performed across multiple states. In general, the above achievable schemes may not be optimal. Hence, we also derive an outer bound on the secrecy capacity region, which is given in the following theorem.
Theorem 4: For the no collaborative eavesdropping model, an outer bound on the secrecy capacity region of the fading broadcast channel is given by

$$\bar{\mathcal{R}}_s = \bigcup_{p(\underline{h})\in\mathcal{P}} \left\{ \begin{array}{l} (R_1,\ldots,R_K): \\ R_i \le \min\limits_{j\neq i, 1\le j\le K} E_{\underline{h}\in \bar{\mathcal{A}}_{ij}}\Big[\log\left(1+p(\underline{h})|h_i|^2\right) \\ \qquad\qquad - \log\left(1+p(\underline{h})|h_j|^2\right)\Big] \\ \text{for} 1\le i\le K \end{array} \right\} \quad \ldots\ldots\ldots(14)$$

Where

$$\bar{\mathcal{A}}_{ij} = \left\{\underline{h} : |h_i|^2 \ge |h_j|^2\right\} \quad \ldots\ldots\ldots\ldots\ldots\ldots(15)$$

and the secrecy rate vector R[t] is chosen to be a solution to the following optimization problem:

$$\max_{p(\underline{h})\in\mathcal{P}}\Bigg[q_1[t]\min_{j\neq 1,1\leq j\leq K}\{R_{1j}(\underline{h})\}+\cdots +q_K[t]\min_{j\neq K,1\leq j\leq K}\{R_{K,j}(\underline{h})\}\Bigg] \quad \text{.....(16)}$$

Proof: The proof is similar to the proof of Theorem 4 given in Appendix D, and is hence omitted. *Remark :* Based on an improved secrecy rate region given in (14), the joint design for stability in Theorem 4and utility maximization in Theorem 5 also needs to incorporate state allocation at the physical layer, which determines the achievable rate vectors jointly with power control.

4. CONCLUSION

The approach in this paper can be applied to analyze other wireless networks including Multiple-access, interference, and relay networks. This approach also allows the incorporation of public and common message flows for users in the system as well. we developed, and implemented a compromised router detection protocol (DP) that dynamically infers, based on measured traffic rates and buffer sizes, the number of congestive packet losses (CPL) that will occur. Each and every packet is encrypted so that to prevent the data from eavesdropping. So the data is much secured. Once the ambiguity from congestion is removed, subsequent packet losses can be attributed to malicious actions, still existing system is a good experiment but it will take more time while it's in the process. So to overcome this along with the queue method by proposing shortest seek first algorithm (SSFA) for the better results to overcome the draw back of lacking time.

REFRENCES:

[1] M. Neely, E. Modiano, and C. Li, "Fairness and optimal stochastic control for heterogeneous networks," in Proc. IEEE INFOCOM, Miami, FL, Mar. 2005, vol. 3, pp. 1723–1734.
[2] A. Stolyar, "Maximizing queueing network utility subject to stability: Greedy primal-dual algorithm," Queueing Syst., vol. 50, no. 4, pp. 401–457, Aug. 2005.
[3] A. Eryilmaz and R. Srikant, "Joint congestion control, routing and MAC for stability and fairness in wireless networks," IEEE J. Sel. Areas Commun., vol. 24, no. 8, pp. 1514–1524, Aug. 2006.
[4] M. Bloch, J. Barros, M. R. D. Rodrigues, and S. W. McLaughlin, "Wireless information-theoretic security," IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2515–2534, Jun. 2008.
[5] E. Ekrem and S. Ulukus, "Degraded compound multi-receiver wiretap channels," IEEE Trans. Inf. Theory, 2009, submitted for publication.
[6] E. Ekrem and S. Ulukus, "The secrecy capacity region of the Gaussian MIMO multi-receiver wiretap channel," IEEE Trans. Inf. Theory, vol. 57, no. 4, pp. 2083–2114, Apr. 2011.
[7] E. Ekrem and S. Ulukus, "Secrecy capacity of a class of broadcast channels with an eavesdropper," Special Issue on Wireless Physical Layer Security, EURASIP J. Wireless ommun. Netw., vol. 2009, pp. 29–29, 2009, Article ID 824235.
[8] E. Ekremand S. Ulukus, "Ergodic secrecy capacity region of the fading broadcast channel," in Proc. IEEE Int. Conf. Commun. (ICC), Dresden, Germany, 2009.
[9] E. Ekrem and S. Ulukus, "Capacity region of Gaussian MIMO broadcast channels with common and confidential messages," IEEE Trans. Inf. Theory, 2010, submitted for publication.
[10] P. Gopala, L. Lai, and H. E. Gamal, "On the secrecy capacity of fading channels," IEEE Trans. Inf. Theory, vol. 54, no. 10, pp. 4687–4698, Oct. 2008.
[11] A. Khisti, A. Tchamkerten, and G. Wornell, "Secure broadcasting," Special Issue on Information Theoretic Security, IEEE Trans. Inf. Theory, vol. 54, no. 6, pp. 2453–2469, Jun. 2008.
[12] Z. Li,W. Trappe, and R.D. Yates, "Secret communication viamulti-antenna transmission," in Proc. Conf. Information Sciences and Systems (CISS), Baltimore, MD, Mar. 2007.
[13] A. D. Wyner, "The wire-tap channel," Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Oct. 1975.
[14] I. Csiszár and J. Körner, "Broadcast channels with confidential messages," IEEE Trans. Inf. Theory, vol. IT-24, no. 3, pp. 339–348, May 1978.
[15] Y. Liang, H. V. Poor, and S. Shamai (Shitz), "Information theoretic security," in oundations and Trends in Communications and Information Theory. Hanover, MA: Now Publishers, 2008, vol. 5, nos. 4–5, pp. 355–580.

BIBLOGRAPHY:

Mr.MD SIRAJUL HUQUE received his B.Tech in Computer Science & Engg from Nimra College of Engg & tech,JNTU Hyderabad.Pursuing M.tech in Computer science & engg from NCET,Vijayawada affliated to JNTUK. he has 5+ years of teaching Experience.He is working as Assistant Professor in St.Anns College of Engg & Tech,Chirala Affliated to JNTUK.

Perusing M.tech (CSE) in Nimra Institute of Science &technology(NIST).

AThirupathaiah received M.tech(IT) from Punjabi University in Nov 2003,Patiala.He worked as a Assoc. Professor in St.Anns college of engineering & Technology, in the period of (2008-2010).He is currently pursuing M.tech in computer science & engineering at St.Anns college of Engg. & technology which is affiliated under the JNTU, Kakinada. He is member of CSI and MISTE .He has total of 11 years of experience in Teaching field. He is a Life time Member of ISTE and CSI. His area of
interests are Computer Networks , Network Security and Cloud Computing..

