12-19-2008

Cooperative Jamming in Wireless Networks - Turning Attacks into Privacy Protection

Jingqi Wu
University of New Orleans

Cooperative Jamming in Wireless Networks - Turning Attacks into Privacy Protection

A Thesis

Submitted to the Graduate Faculty of the
University of New Orleans
in partial fulfillment of the
requirements for the degree of

Master of Science
in
Computer Science
Systems and Networks

by

Jingqi Wu

B.S. Zhejiang University, 2000
M.S. Zhejiang University, 2003

December, 2008

Acknowledgment

I would like first to thank the students in our research group for the selfless help they provided. In particular, thanks to Zhiguo Zhang and Kejun Liu. They have being helping me when there are research problems. We discussed together about any interesting research topics in the field of wireless communication. Inspirations are usually generated in brain storm. I enjoyed very much when talking or even arguing on research problems with them.

Dr. Deng helped me greatly. He used his funding to support me. Actually my wife and I both lived on his support, with which I did not need to worry too much about the financial problems. Moreover, Dr. Deng also acted as my professor before he finally left University of New Orleans. Wireless Networks is one of his research fields. In this field he has already done a lot of work and published many papers for conferences and journals. It is always a happy time to take his classes and have regular meetings with him. Whenever I met with hard questions, Dr. Deng was the best person to look for an answer. As the research work went go, Dr. Deng gave me different chances to show my research results. I was encouraged to give my seminar, which improved my ability of giving a talk.

I am very grateful to Dr. Vassil, Dr. Tu and Dr. DePano for attending my master's thesis committee. They guided me through the writing of this thesis, and made sure that my thesis can meet the requirements of the research depth and breadth. It is their supervision that guaranteed the quality of my research and my thesis.

Our department chair, Dr. Mahdi, is another person that I owe a lot. As the department was recovering from the Katrina, Dr. Mahid did much to keep the stability of the department and tried his best to protect the students from various problems. I felt lucky that I had a good environment to study and research.

The last one is the most important one. She is like an angel protecting me from famine and loneliness. Whenever I get depressed she is able to encourage me. Thanks a lot to my wife, You Lin, for coming to USA with me and leaving her home town. Although she is not able to help me on my research, I can hardly live a day without her in my life.

Table of Contents

Abstract

Generally, collisions between packets are undesired in wireless networks. We design this scheme, Cooperative Jamming in Wireless Networks (CJWN), to make use of collision to protect secret DATA packets from being sniffed by a nearby eavesdropper. We are intending to greatly increase the Packet Error Rate (PER) at the eavesdropper when the PER at the receiver is maintained at an acceptable level. This scheme is not intended to completely take the place of various encryption/decryption schemes which are working based on successfully received packets. Adding CJWN to the popular CSMA/CA adopted in IEEE 802.11 will add more security even the key for encryption/decryption is already exposed. Because the overhead of CJWN is very big, we do not suggest using it on every transmission. When some secret packets have a high requirement of confidentiality, CJWN is worth trying at the cost of throughput performance and power.

Keywords:

Wireless Communication, Propagation Model, 802.11b, MAC, CSMA/CA, CJWN

Introduction

The first two subsections of this section are the two aspects that are to be brought together in this thesis. Here are brief introductions of them. I will discuss them in the following sections in more detail.

Wireless Communication

Since Guglielmo Marconi demonstrated the ability of radio to support the continuous contact between the sailing ships across the English Channel, it has evolved greatly for moving people to communicate with each other. Wireless communication is the transfer of information over the air without the help of any electrical conductors such as wires. There is no limitation for the range of the distance between partners. It can be short like television remote control within a few meters, and it also can be very long like satellite telephone which sends signal over thousands of kilometers.

There are many applications of wireless communications around us. Cell phone and Walkie-talkie are two typical instances with and without infrastructures. Some of our personal digital assistants (PDAs) and laptops are already integrated with WiFi and Bluetooth. GPS units help us find the way. Even our garage door can be equipped with wireless opener.

New wireless communication methods and services are enthusiastically adopted by people throughout the world. It is particularly obvious during the past ten years. The mobile radio communication industry has grown by orders of magnitude 0. As the improvements of digital, radio frequency (RF) circuit, new large-scale circuit integration and other miniaturization technologies, people have made portable radio equipment smaller, cheaper and more reliable.

There are two fundamental aspects of wireless communication that make the problem challenging and interesting [2]. Also the two aspects are the two important differences between wireless communication and its wired sibling. Fading is the first one, and it represents the time variation of the channel strengths due to the small-scale effect of

multipath fading and large-scale effects such as path loss with distance attenuation and shadowing by obstacles. The second one is interference. In the wired world each transmitter-receiver pair can generally be thought of as isolated point-to-point link. But wireless communications nearby will cause significant interference among them. The common transmission medium makes it extremely hard to prevent interference. Thus, how to deal with fading and with interference is the central to the design of wireless communication systems.

Security Problem

The security problem in wireless communication is basically the prevention of unauthorized access or damage to computers using wireless networks [3].

The principles of security problem include Confidentiality, Integrity, Authentication, Availability, Non-repudiation. These are usually abbreviated as CIAAN.

Confidentiality means the protections against the disclosure of information to parties other than the intended recipients. It is often ensured by means of encoding the information using an algorithm and a secret. The secret is known only to the originator of the information and the intended recipients (cryptography). The two meanings of confidentiality are the confident data or the fact that they are talking to each other. The choices of protection for confidentiality are protecting encryption scheme (whatever way the sender mingles the data) and protecting secret (shared secret between sender/receiver).

Integrity allows the receiver to confirm that the received information has not been altered in transit or by third party. Sometimes it uses similar approach as confidentiality schemes, but usually it pads additional information as Message Authentication Codes (MAC).

Authentication establishes the validity of a transmission, a message or the originator. It makes sure that the information was sent from a claimed source by detecting spoofing. Digital certificates, digital signatures and biometrics are examples of the methods used to guarantee authentication.

Availability assures information and communication services ready for use as expected. Service is supposed to be available to authorized users when they need it. A typical attack against availability is Denial of Services (DoS) or Distributed DoS (DDoS). The methods used for availability include redundancy, replica, backup, etc.

Non-repudiation prevents later denial that an action happened, or a communication that took place. It usually includes interchanges of authentication information combined with some form of provable time stamp. Fraud and repudiation of transactions are the attacks to Non-repudiation, and measures taken against them are Public Key Infrastructure (PKI) and digital signatures.

The Goals of this Thesis

Facing with the vulnerabilities of wireless communication and the potential attacks to security principles of CIAAN, people are doing research to make wireless more stable and more secure. My thesis is aiming at strengthening the confidentiality of wireless communication. That scheme is different from the regular schemes of cryptography, and it does not rely on keys to encrypt and decrypt the messages. The point of our Cooperative Jamming in Wireless Network (CJWN) scheme is actually trying to attack the attackers by breaking their availability. CJWN makes use of attacking method to protect ourselves from being attacked. It is an active way rather than passive schemes of cryptography. In this thesis I will introduce the application background of our scheme, the propagation model, the basic idea of CJWN, the analysis of CJWN performance and practical approach of CJWN. Furthermore I will introduce the related work of CJWN, present my thinking of the future work of my research, and finally I will come up with a conclusion of CJWN scheme and my research work.

Another important goal of this thesis is to inspire people to look at the security problem from a different perspective. From this special perspective of active protection, people may find completely different ways to fix or at least alleviate the attack to our wireless communication.

Structure of the Text

The whole text is organized in the following way. I will first give an introduction of the wireless communication. Besides the basic conception of wireless communication, I will go into the propagation models of electromagnetic waves, which is the basic of my analysis of the CJWN scheme. Also, IEEE802.11 and CSMA/CA are also introduced in detail because our CJWN is actually making modification to CSMA/CA to make it applicable with the message protection.

After that I will come to the CJWN scheme. Background of the CJWN is first presented, and then some related work is also discussed. The research outcome from other researchers can not only give us a review but also give us a chance to compare the CJWN with other schemes. Because the analysis of CJWN is related with many practical parameters in wireless communication, we will introduce the system models and parameter selection. The mechanism of CJWN scheme follows immediately. The layout of nodes distribution and the aggregation of CSMA/CA and CJWN are discussed in detail. Then we evaluate the performance of CJWN proving the effectiveness of CJWN. In order to make CJWN more practical, we further give an alternative approach which is easier to carry out and more accurate.

Finally I draw a conclusion of my research work and introduce the future work which is interesting and promising.

Wireless Communication

Basics of Wireless Communication

A computer network is an interconnected collection of independent computers which aids communication in numerous ways. A modern-day computer consists of two major components, namely, distributed applications and network infrastructure [4]. The distributed applications provide services to users/applications located on other computers. The most popular instances of such application include HTTP web browsing, electronic mail, voice over IP, etc. Normally, there should not be any restrictions on the physical media used for providing connectivity among terminals. For the wired networks, the most common medium are copper cable, optic fiber. On the other hand, the wireless networks share the space as the unique medium. My thesis focuses on wireless networking, and ad hoc wireless networks in particular.

Wireless communications is based on the principles of broadcast and reception of electromagnetic waves. The frequency (f) of these waves indicates the cycles every second, and it is measured in Hertz (Hz). We can also use the wavelength (λ) to characterize these waves. Wavelength means the length the wave can travel every second in vacuum. The relation between f and λ can be given as Eq(1) where c is the speed of light ($3\times10^{8} m/s$), f is in Hz and λ is in meter.

$$c = \lambda \times f \tag{1}$$

Electromagnetic waves of different frequencies are usually assigned for different bands and different usages. Here is a table to show the name, frequency and typical applications of these bands Table 1.

Band Name	Frequency	Typical Applications
Extremely Low Frequency (ELF)	30 to 300 Hz	Powerline frequencies
Voice Frequency (VF)	300 to 3,000 Hz	Telephone communications
Very Low Frequency (VLF)	3 to 30 KHz	Marine communications
Low Frequency (LF)	30 to 300 KHz	Marine communications
Medium Frequency (MF)	300 to 3,000 KHz	AM broadcasting
High Frequency (HF)	3 to 30 MHz	Long-distance aircraft/ship communications
Very High Frequency (VHF)	30 to 300 MHz	FM broadcasting
Ultra High Frequency (UHF)	300 to 3,000 MHz	Cellular telephone
Super High Frequency (SHF)	3 to 30 GHz	Satellite communications, microwave links
Extremely High Frequency (EHF)	30 to 300 GHz	Wireless local loop
Infrared	300 GHz to 400 THz	Consumer electronics
Visible Light	400 THz to 900 THz	Optical communications

Table 1 Frequency bands and common uses

For both indoor and outdoor communication, Radio waves are easy to generate and are widely used due to the properties such as the ability to pass through buildings and ability to travel long distances. Different bands have different ability to go through obstacles. We are going to talk about it in next section. Except the transceivers using directional antennas, radio transmission is omnidirectional (when radio waves are generated, they spread out from the transmitting antenna in all directions) in nature. The waves are easier to pass through obstacles when the frequency is lower. Meanwhile, the power also falls with an inverse-squared relation (free space propagation model) with respect to the distance. As the frequency grows higher, the waves are more prone to the absorption by small obstacles, like rain drops, and get reflected by big obstacles, like walls.

Some bands of waves are called ground waves because they follow the curvature of the Earth and they can reach the maximum ranges of a few hundred kilometers. Some other bands of the radiation are called sky wave. They radiate outward to the ionosphere in the upper atmosphere, which reflects the sky wave back to the Earth. If the power is strong enough, sky wave can reflect several times between the Earth and the ionosphere. In the SHF band, microwave transmissions tend to travel in straight lines and can be narrowly focused. Microwave can be used for mobile phones and television transmission since the energy is concentrated leading to a higher signal-to-noise ratio (SNR, the ratio of the signal power to the noise power). The shortcoming of microwave is that it can't pass through buildings. So repeaters are required for long distance transmission. Waves in the EHF band and infrared waves are only used for short-range communication like the remote controls of television, VCR and stereo remote controls. They travel like visible light and go pass no obstacles.

In wireless communication there is another important aspect, spectrum allocation. It is because the electromagnetic spectrum is actually a common resource. It is open to every user. If people do not put regulation on the usage of the spectrum, much more interference and collision will be inevitable. The typical applications of each band are already shown in Table 1. The International Telecommunications Union Radiocommunication (ITU-R) Bureau tries to coordinate the spectrum allocation by the various national governments. The simplest method of allocating frequencies is not to allocate them at all. So ITU has designed some frequency bands, called the ISM (industrial, scientific, medical) bands, for unlimited usage. These bands commonly used by wireless LANs and PANs are around the 2.4 GHz band. Parts of the 900 MHz and the 5 GHz bands are also available for unlicensed usage in countries such as the United States and Canada. The most popular MAC protocol for wireless LANs is IEEE802.11b. IEEE802.11b also works in ISM bands and it supports the ad hoc working mode. CJWN is based on IEEE802.11b and ISM band.

Propagation Models

Factors Affecting the Signal Propagation

The fundamental limitations on the performance of wireless communication are caused by the mobile radio channel. The radio signal can travel by simple line-of-sight path if there is any, and it may also be reflected multiple times by buildings, mountains and foliage. Wired channels are usually more stable and robust than wireless channels. By constraining the signal in cable or optic fiber, wired channels are stationary and predictable. On the contrary, radio channels are extremely random and do not offer easy analysis. Not only the physical environment but also the moving speed of the sender and receiver will impact how rapidly the signal level fades.

There are many kinds of factors behind electromagnetic wave propagation. But most of them can be classified into three categories. They are reflection, diffraction and scattering. When the propagating radio wave hits an object which is very large compared to its wavelength, the wave gets reflected by that object. Reflection causes a phase shift of 180 degree between the incident and the reflected rays. Diffraction is undergone by a wave when it hits an impenetrable object. The wave bends at the edges of the object, thereby propagating in different directions. The dimensions of the object causing diffraction are comparable to the wavelength of the wave. The bending causes the wave to reach places behind the object which are out of the line-of-sight transmission. Scattering happens when the wave travels through a medium, which contains many objects with dimensions small compared to its wavelength. The wave gets scattered into multiple outgoing signals. Figure 1 shows the different propagation mechanisms.

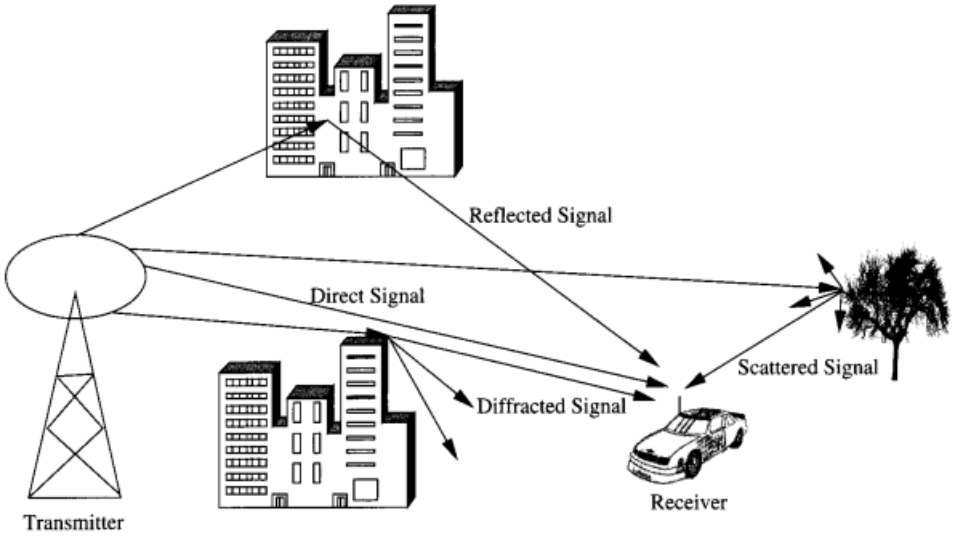

Figure 1 Propagation mechanisms

In urban areas there is typically no direct line-of-sight path between the transmitter and the receiver, and the presence of high-rise buildings causes severe diffraction loss. Because of the multiple reflections from various objects, the electromagnetic waves travel along different paths of varying lengths. Finally these waves will interact causing multipath fading at a specific location. Basically the strengths of waves will decrease as the distance increases between the sender and receiver.

Large-Scale Propagation and Small-Scale Fading Models

The propagation models can be roughly categorized into large-scale propagation models and small-scale or fading models. Large-scale propagation models predict the mean strength for an arbitrary sender-receiver distance. Small-scale or fading models characterize the rapid fluctuations of the received signal strength over very short travel distances (a few wavelength) or short time durations (on the order of seconds) [4]. The relation between the two models can be roughly shown in Figure 2.

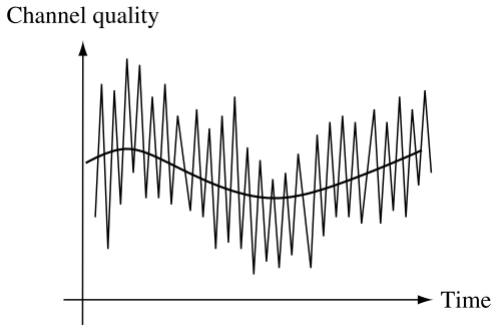

Figure 2 Channel quality varies multiple time-scales. At a slow scale, channel varies due to large-scale fading effect. At a fast scale, channel varies due to multipath effects.

The instantaneous received signal strength may fluctuate rapidly when a mobile moves over very small distance. It is because that the received signal is a summation of many components from multiple directions. The phases of these components are random, so it is hard to say they will strengthen each other or simply cancel out. Small scale fading may cause up to 30 or 40 dB magnitudes when the receiver is moved by only a fraction of a wavelength. Large-scale propagation models predict the local average signal level when the mobile moves away from the sender over much larger distances.

The typical model of large-scale propagation models is the free space propagation model. In this model the relationship between the transmitted power P_t and the received power P_r is given by Eq(2).

$$P_r = P_t G_t G_r (\frac{\lambda}{4\pi d})^2 \qquad (2)$$

G_t and G_r are the transmitter and receiver antenna gains. Antenna gain is defined as the ratio of the power required at the input of a loss-free reference antenna to the power supplied to the input of the given antenna to produce, in a given direction, signals of the same strength at the same distance. D is the distance between the transmitter and receiver.

The free space model described above assumes that there is only one single path from the transmitter to the receiver. But when we consider some more realistic environment, the signal reaches the receiver through multiple paths. There are possibly reflection,

refraction and scattering. Therefore we use another large-scale propagation model, the two-path model, to capture this phenomenon. This model is applicable when the signal reaches the receiver through two paths. One path is the line-of-sight path, and the other path is for the reflected, refracted or scattered wave. Based on the two-path model, the received power is calculated by Eq(3).

$$P_r = P_t G_t G_r (\frac{h_t h_r}{d^2})^2 \tag{3}$$

Besides the parameters existing in free space model, h_t and h_r are the heights of the sender and the receiver, respectively.

More generally, for isotropic antennas (antennas in which the power of the transmitted signal is the same in all directions), the received power of the signal is given by Eq(4)

$$P_r = P_t G_t G_r (\frac{\lambda}{4\pi})^2 \frac{1}{d^\gamma} \tag{4}$$

In this equation, γ means the propagation coefficient. It usually varies from 2 (free-space propagation) to 5 (strong attenuation).

The Equations of (2), (3) and (4) is not applicable when d is close to 0, because the received power P_r will not be infinite. They are only effective when the distance between sender and receiver is bigger than Fraunhofer region d_f. d_f must meet Eq(5), (6) and (7).

$$d_f = \frac{2D^2}{\lambda} \tag{5}$$

$$d_f >> D \tag{6}$$

$$d_f >> \lambda \tag{7}$$

D is the largest physical linear dimension of the antenna.

IEEE802.11 and CSMA/CA

IEEE802.11

The Institute of Electrical and Electronics Engineers (IEEE) provided several standards for LANs. The IEEE 802 standards form a collection each of which defines one aspect for the local area networks. Table 2 gives the list of protocols and their definitions.

Protocol	Definition
802.1	internetworking
802.2	logical link control
802.3	Ethernet or CSMA/CD
802.4	token bus LANs
802.5	token ring LANs
802.6	MANs
802.7	broadband LANs
802.8	fiber optic LANs
802.9	integrated (voice/data) services LANs and MANs
802.10	security in LANs and MANs
802.11	wireless LANs
802.12	demand priority access LANs
802.15	wireless PANs
802.16	broadband wireless MANs

Table 2 802 protocols and their definitions

The content of IEEE802 standard only contains the regulation of the data link layer and the physical layer of the OSI reference model.

The responsibility of physical layer is to deal with the raw bits to transmit or receive. It is responsible for the bit encoding, determining the voltage to be used for the 0/1 bit transmissions, and the time duration of each bit. Therefore, the implementation of the physical layer varies depending on the physical medium used. The popular physical transmission media are twisted pair, coaxial cable, optical fiber, and radio waves.

The MAC layer is the sub layer of the data link layer, and MAC layer uses the services from the physical layer. The LLC layer is also a sub layer of the data link layer, and LLC is actually residing above the MAC layer. So LLC layer directly uses the services from MAC layer. This structure is shown in Figure 3. My thesis will focus on the MAC layer.

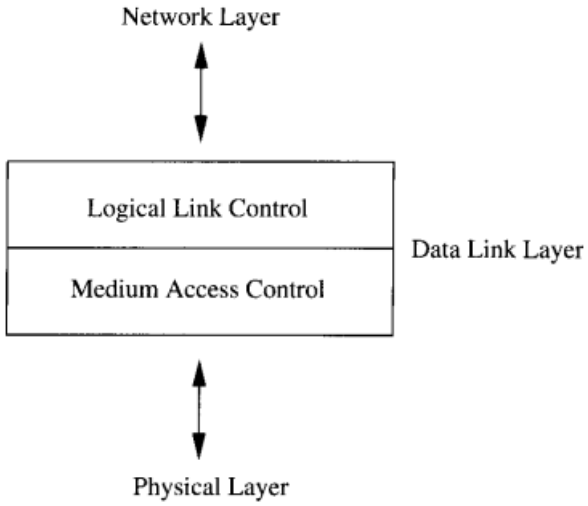

Figure 3 Data link layer

To wireless communication users, 802.11b is the most familiar part. But each task group of 802.11 has its specific responsibility as show in Table 3.

task group	responsibility
802.11	To develop MAC layer and physical layer specifications for wireless connectivity for fixed, portable, and mobile nodes within a local area.
802.11a	To create a standard for wireless LAN operations in the 5 GHz frequency band to support a data rate of up to 54 Mbps.
802.11b	To create a standard for wireless LAN operations in the 2.4 GHz ISM band. It is popularly referred to as Wi-Fi.
802.11c	To devise standards for bridging operations for bridges and access points.
802.11d	To publish definitions and requirements for enabling the operation of the 802.11 standard in countries that are not currently served by the standard.
802.11e	To define an extension of the 802.11 standard for quality of service (QoS) provisioning and service differentiation in wireless LANs.

Table 3 Various 802.11 task groups and their responsibilities

(table continued)

802.11f	To develop specifications for implementing access points and distribution systems following the 802.11 standard, so that interoperability problems between devices manufactured by different vendors do not arise.
802.11g	To extend the 802.11b standard to support high-speed transmissions of up to 54 Mbps in the 5 GHz frequency band, while maintaining
802.11h	To supplement the 802.11 standard in order for the MAC layer to comply with European regulations for 5 GHz wireless LANs.
802.11i	To enhance security in the 802.11 standard.
802.11j	To enhance the current 802.11 MAC physical layer protocols to additionally operate in the newly available Japanese 4.9 GHz and 5 GHz bands.
802.11n	To define standardized modifications to the 802.11 MAC and physical layers such that modes of operation that are capable of much higher throughputs at the MAC layer, with a maximum of at least 100 Mbps, can be enabled.

Previous MAC protocols

The first MAC protocol for wireless communication is ALOHA. The pure ALOHA system is very simple. A terminal is allowed to transmit data whenever data is ready. Obviously, if more than one user transmits simultaneously, the packets will collide with each other ending resulting in nothing transmitted.

Without any mechanism to control the access to the public medium, pure ALOHA can only achieve relatively low throughput. Slotted ALOHA is an advanced version of ALOHA. It requires the channel to be divided in time into discrete intervals/slots. Each slot has a length equal to the length of the data frame. All the nodes have the same boundaries of slots and they are synchronized. Slotted ALOHA does not allow nodes to send packet at will. Instead, they wait until the beginning of the next slot interval and then transmit. If the transmitted frame gets collision, nodes are required to wait for a random period of time, and the retransmissions are scheduled at the beginning of the next interval.

Because of wastage of bandwidth due to packet collisions, the maximum achievable throughput of the ALOHA protocols is relatively low. Carrier sense multiple access (CSMA) protocols enforce the nodes to first listen for a carrier (transmission) on the channel, and make sure there is no on-going transmission, before they can actually start their own packets transmission.

Several CSMA protocols are adopted. 1-persistent CSMA is one of them. In this protocol, a node first senses the channel to see if the channel is free. Packet is transmitted at once when the channel is free. If the channel is not free, the node will keep on sensing the channel until the channel is free again. Because the probability that a ready node starts transmitting once it finds the free channel is 1, we call it 1-persistent CSMA. In resolving collisions between packets, the propagation delay plays an important role. Because of the propagation delay, one node can't sense the carrier from a neighbor node before it starts its own transmission. Then collision happens. So the 1-persistent CSMA scheme performs well when the propagation delay is relatively low.

Then people have the non-persistent CSMA scheme. In non-persistent CSMA scheme, a ready node also senses the channel. The node simply goes into a wait state when a busy channel is found. In the wait state, the node does not sense the channel. The wait period is randomly chosen. When the wait period expires, the node senses the channel again to repeat the algorithm. Quite different from the high collision rate of 1-persistent CSMA, the probability of collisions is lowered a lot when nodes wait for different randomly chose time periods before sensing the channel again.

p-persistent CSMA combines the best features of the above two schemes. Just like slotted ALOHA scheme, p-persistent CSMA has the channel slotted. A ready node will first sense the channel. If an idle slot is sensed, it uses the same slot with p as the probability, or defers the transmission to the next idle slot with probability q = 1-p. Once the next idle slot comes, the node will again transmit or defer the transmission with the probability of p and q. The values of p and q are the key of the performance of p-persistent CSMA, and they are quite related with the load of the networks.

Based on the CSMA schemes, people developed CSMA with collision detection (CSMA/CD). CSMA/CD is only applicable in wired networks because only in wireless

networks can the nodes detect a collision on the channel. We are not going to discuss much into CSMA/CD, but we are going to focus on its sibling in wireless networks.

The IEEE802.11 standard is one of the most popular standards for wireless LANs. It specifies the physical layer and the MAC layer, adapted to the specific requirements of wireless LANs.

There are three different physical layers supported by basic 802.11 standard. Frequency hopping spread spectrum (FHSS) and direct sequence spread spectrum (DSSS) are two of them and they are based on radio transmissions. The third one is clear channel assessment (CCA). CCA is based on infrared, and it provides mechanisms for sensing the wireless channel and determining whether or not it is idle.

In the MAC layer, carrier sense multiple access with collision avoidance (CSMA/CA) is adopted by the 802.11 standard. As I mentioned above, because of the nature of the radio environment it is very difficult for a transmitting node to detect packet collisions in the networks. Therefore, CSMA/CD is definitely not applicable in wireless LANs.

CSMA/CA

The primary access method of IEEE802.11 is by means of a distributed coordination function (DCF). This mandatory basic function is based on a version of CSMA/CA. an optional RTS-CTS mechanism is implemented to avoid the hidden terminal problem (explained later). Another method called the point coordination function (PCF) is implemented to provide real-time services. In PCF mode, the AP controls medium access and avoids simultaneous transmissions by the nodes. The ad hoc networks are based on the DCF because there is no infrastructure in the networks.

Now here are the details of CSMA in IEEE802.11 DCF. Figure 4 shows the basic channel access mechanism of IEEE802.11.

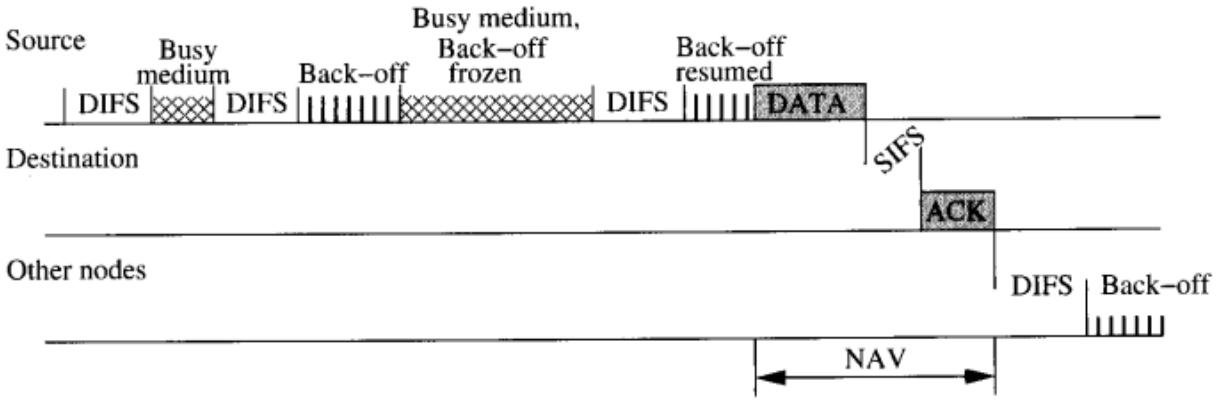

Figure 4 Basic channel access mechanism of IEEE802.11 [4]

If the node senses medium to be free for more than the duration of DCF inter-frame spacing (DIFS), the node will access the medium for transmission. If the mediums is busy, the node will back off. Backing off means the node defers channel access by a random amount of time chosen within a contention window (CW). $CW_{\min}$ and $CW_{\max}$ are the minimum and maximum value of the CW. CW can only be chosen from integral multiples of slot times. These values of CW are judiciously picked using propagation delay. The node will back off until the back-off counter reaches zero and expires, and then the node can access the medium. Unfortunately, if the node detects a busy channel during its back-off process, the node will freeze the back-off counter and the process is resumed once the channel becomes idle for a period of DIFS. For every transmission, the sender will experience the back-off procedure at least once. Instead of choosing another random interval from the contention window, longer waiting stations will wait only for a residual amount of time that is specified by the back-off timer. The reason of this behavior is very important and can be explained as following. If each station has the same chances for transmitting data next time regardless of the overall waiting time that has been experienced by each node, it is clearly unfair. We would like to give the long waiting nodes much more chance or higher priority to use the channel.

Acknowledgements (ACKs) are required for data packets to make sure the correct delivery of the data packets. Of course, the ACK packets are only necessary in unicast situations. The receiver will first check if the data packet is correctly received, then the receiver will wait for an SIFS and the sends back the ACK packet. Other nodes have to wait at

least DIFS and a back-off time before they can access the channel. Therefore, a higher priority is given to the receiver to send an ACK.

In CSMA, there exists a big short-coming called hidden-terminal problem. Hidden-terminal problem is shown in Figure 5.

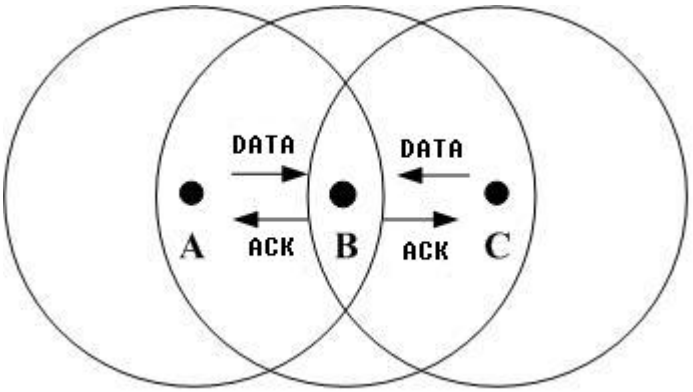

Figure 5 Hidden terminal problem

When A sends DATA packet to B, C is not able to sense the carrier signal on the channel because C is out of the transmission range of A. Therefore C will also start its transmission to B on the “idle” channel. The result will simply be a packet collision at B.

Another big problem in CSMA is the, so called, exposed terminal problem. As shown in Figure 6, B is sending A a DATA packet. C also wants to send its DATA packet to D after B has already started the transmission. Obviously C will sense a busy channel, and then refrain from sending anything to D. But this is actually a wasting of the channel because the DATA packet from C will not reach A for that long distance.

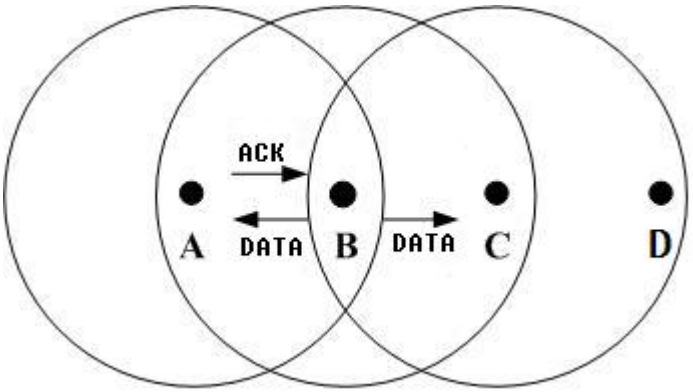

Figure 6 Exposed terminal problem

In order to solve (at least alleviate) both the hidden terminal problem and exposed terminal problem, people add the RTS-CTS mechanism to CSMA, which finally leads to the CSMA/CA protocol. CSMA/CA is shown in Figure 7.

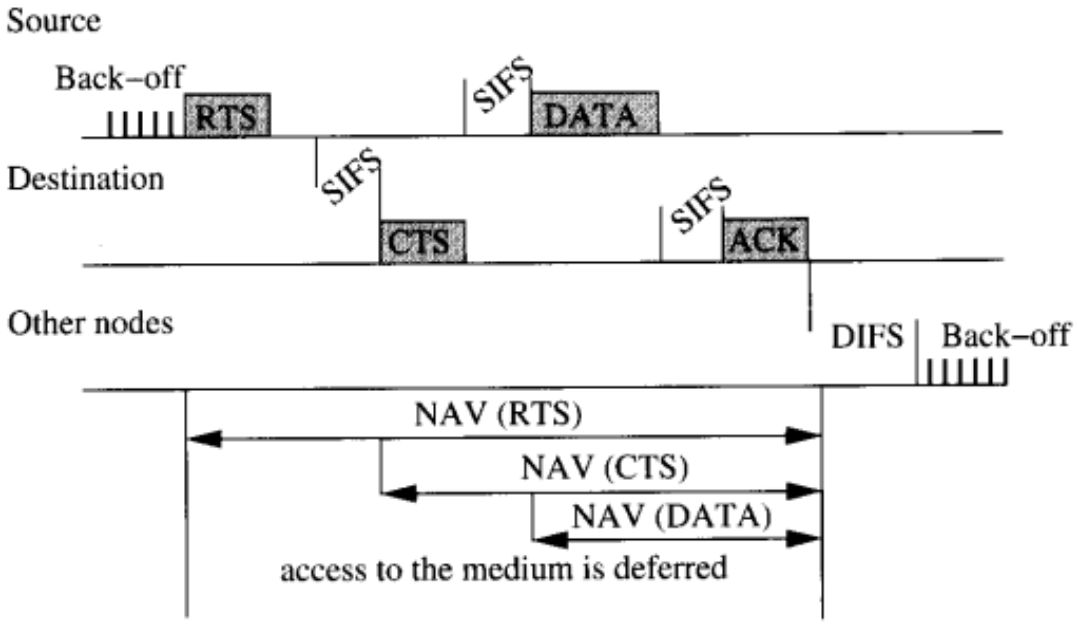

Figure 7 RTS-CTS mechanism

The RTS-CTS mechanism will require the sender send a request to send (RTS) packet to the receiver. The contents of RTS packet include the intended receiver and the expected duration of the whole data transmission. Not only the intended receiver but also all the other nodes in the neighborhood of the sender will hear (if it does not get collided) the RTS packets. Then the third parties will set their network allocation vector (NAV) according to the duration contained in the RTS packet. The NAV of a node specifies the earliest time that the node is allowed to attempt a transmission. The intended receiver will check if its NAV and its channel allow it to receive the coming DATA packet.

If condition allows, receiver will reply with a clear to send (CTS) packet. The contents of CTS packet include the intended sender and the duration field. Of course the duration in CTS is smaller than the duration in RTS. The difference is $T_{SIFS} + T_{CTS}$. The nodes in the neighborhood of the receiver will also update their NAV according to the duration in the CTS packet. Now both the nodes in sender's transmission range and nodes in receiver's transmission are informed of the duration of the coming data transmission.

For the problem of the hidden terminal, C in Figure 5 can hear the CTS from B. Then it will not start its transmission because C knows B is busy with another data transmission. For the problem of the exposed terminal, C can hear RTS from B but can't hear the CTS from A. So C believes either A does not reply with CTS to B or A is out of C's transmission range. For both of the two possibilities, C can safely start its transmission with D. Now we have successfully solved the two problems.

After the RTS-CTS mechanism, there follows the DATA packet and the ACK packet. It is same with the CSMA. The usage of RTS-CTS dialog before DATA packet transmission is a form of virtual carrier sensing. We must notice that the RTS-CTS mechanism will bring extra overhead to the sender and receiver. So an RTS threshold is used to determine whether to start the RTS-CTS mechanism or not. If the DATA packet size is bigger than the RTS packet, the RTS-CTS mechanism is required. Otherwise, the transmission will start with DATA packet directly.

CJWN scheme

Background of CJWN

Security is much more important to wireless network than its wired sibling [5]. This is because wireless network uses open medium and it is much easier for an unauthorized node to eavesdrop the on-going communication. The inherent weakness of wireless network gives eavesdroppers more chances, which poses severe problems in military communications. According to this property, distributed security mechanism is more likely to be used in ad hoc networks. As one of the main threats to wireless networks [6], eavesdropping has attracted much attention. Encrypting data is one effective way to keep the information in secret. A robust key exchange and distribution scheme is required and it would also allow revocation of known exposed keys and rekeying of sensor nodes. Usually an end-to-end encryption is impractical when the network contains numerous nodes because a large memory space is required to store the keys for all the nodes and the key exchange for every two nodes is a heavy burden. So people are more likely to adopt hop-by-hop encryption which requires smaller memory space for neighbors' keys and lighter traffic for key exchange.

Besides the encryption, CJWN is trying to protect data packets without relying on the keys. Each node in ad hoc networks requires an acceptable Signal to Interference plus Noise Ratio (SINR) to successfully receive packets. In order to achieve high throughput people usually desire a low addition of interference and noise. IEEE 802.11 [7] adopts Carrier Sense Multiple Access With Collision Avoidance (CSMA/CA) to secure an idle medium environment. It uses not only physical carrier sensing but also virtual carrier sensing by Request To Send (RTS) and Clear To Send (CTS). Multi-Channel schemes can also help mitigate the interference by assigning nearby concurrent transmission into different channels.

Rather than simply pursuing a high SINR, CJWN is designed to decrease the SINR at a node. Obviously it is not beneficial to the receipt of the receiver, but the adverse

eavesdropper will also suffer from the noise. The key to CJWN is to make the eavesdropper have much lower probability of recovering packets from incoming signals when the harm to the receiver is controlled to an acceptable level.

Related Work

In [8], Sinha et al. describes the security threats associated with 802.11 based Wireless Local Area Networks (WLANs) and outlines a comprehensive architecture for a Wireless Intrusion Protection System(WIPS). Most of the threats are also applicable to ad hoc networks. Sniffing can be carried out by hackers using some tools such as Effetch [9], WEPCrack [10] and AirSnort [11]. Moreover, they also produced the AirDefense system to monitor and protect these vulnerable networks around the world. These three sniffing tools require successful signal receipt before they can decode or decrypt them.

0 is the definitive modern text for wireless communications technology and system design. Theodore Rappaport introduces path loss, small-scale fading, multipath, reflection, diffraction, scattering, shadowing, spatial-temporal channel modeling and microcell/indoor propagation for mobile radio propagation models. The propagation models adopted by some simulation tools, such as NS2 [12], are easy to understand and implement. But they are over simplified compared with these realistic models above. Lee [13] et al. propose a realistic transmission range model based on IEEE 802.11a/g. ChSim [14] is a useful component of OMNeT++. The simulator includes several mobility and channel models which consider time and frequency selective fading using Clarke's model [15] assuming an isotropic antenna gain pattern. Path loss and shadowing are included using standard modeling assumptions [16].

In [17], Carlson et al. suggest a new reservation protocol, called JamTDMA. It offers protection against the interference from nearby nodes by advertising the reservations in a larger neighborhood. The analysis and the simulation result show that this protocol allows to improve the rate of successfully received packets while assuring an upper bound for the end-to-end delay. Although CJWN does not have the same purpose as JamTDMA, we are

adopting the similar system models. CJWN is also asking the nodes within certain range of the receiver to keep silence, which is the same requirement of JamTDMA. Additionally, CJWN asks the cooperative nodes to emit noise, which will lower SINR at the eavesdropper.

System Models and Parameter Selection

In our analysis of CJWN scheme, we use the two-path loss model [4]. In this model the relation between the transmitted power P_t and the received power P_r is given by Eq(4). G_t and G_r are the sender and receiver antenna gains, d is the distance between the sender and receiver, and λ is the wavelength of the signal. γ is the propagation coefficient that varies between 2 (free-space propagation) and 5 (strong attenuation). We fix γ at 3 for our analysis. For a simple dipole antenna, an assumption of 1 gain [18] is reasonable. This number will be taken for the gain of both the sender antenna gain (G_t) and receiver antenna gain (G_r). As I have mentioned before, P_r can't become infinity when d is reaching 0. Therefore Eq(4) is only effective in Fraunhofer region, which is beyond far field distance d_f 0. d_f must meet the requirements of Eq(5), (6) and (7). We set $d_f = 1m$. An approximate assumption is that any receiver within distance of d_f will have the received power P_r as if it was exactly d_f from the sender. This little adjustment to the two-path loss model makes the propagation model more practical. The modified model is shown in Eq(8).

$$P_r = \begin{cases} P_t G_t G_r (\frac{\lambda}{4\pi})^2 \frac{1}{d^\gamma} & \text{if} \quad d \geq d_f \\ P_t G_t G_r (\frac{\lambda}{4\pi})^2 \frac{1}{d_f^\gamma} & \text{if} \quad d < d_f \end{cases} \tag{8}$$

Our analysis is based on the modulation of Differential Binary Phase Shift Keying (DBPSK) at 1 MBps (physical layer of IEEE802.11 [7]). Carrier wave is working at $f = 2.4GHz$, Hence $\lambda = 0.125m$ in Eq(4). The transmission power is always set at the maximum value of $P_t = 100\,mW$ [19] when it is sending regular control packets and DATA packets. Meanwhile, we assume that each node has the same capability of emitting radio signal at any power between 0 and P_t. The typical bandwidth BW for DBPSK is 2 times of the bit rate R [18], so $BW = 2 \times 1MBps = 2MHz$. The theoretical noise floor N for an ideal receiver can be calculated as Eq(9).

$$\begin{aligned} N &= kTB \\ &= 1.38 \times 10^{-23} J/K \times 290K \times 2{,}000{,}000Hz \\ &= 8 \times 10^{-15} W \end{aligned} \tag{9}$$

A real receiver noise floor will always be higher due to Noise Figure (NF), the noise and losses in the receiver itself. A typical number for a receiver would be about 7dB. So the practical Receiver Noise Floor (RNF) can be determined as Eq(10).

$$\begin{aligned} RNF &= N \times NF \\ &= 8 \times 10^{-15} W \times 10^{0.7} \\ &= 4 \times 10^{-14} W \end{aligned} \tag{10}$$

Then the receiver's Bit Error Rate (BER) for DBPSK is calculated as Eq(11).

$$\begin{aligned} BER &= \frac{1}{2} e^{-\frac{BW}{R} SINR} \\ &= \frac{1}{2} e^{-\frac{BW}{R} \frac{P_r}{P_i + RNF}} \end{aligned} \tag{11}$$

P_i is the accumulated power of interference. The receiver's Packet Error Rate (PER) is

further calculated as following Eq(12).

$$PER = 1 - (1 - BER)^{psize} \tag{12}$$

In this equation, psize is the length of the DATA packet measured in bits. Normally we can assume the length of the DATA packet to be 2300bytes. Therefore we make $psize = 2300 \times 8bits$. There exists a maximum acceptable PER when two nodes want to create a data link between them. According to the data link budget analysis [18], we can assume a reasonable value, 5%, for the maximum acceptable PER, $PER_{\max}$.

The communication range r_c is the maximum distance where sender and receiver can create a link (in the absence of any interference). Combining Equation (10), (11) and (12), we can calculate the minimum acceptable P_r, $P_{r\min}$.

$$P_{r\min} = -\frac{1}{BW} \times (P_i + RNF) \times R \times \ln(2 \times (1 - (1 - PER_{\max})^{\frac{1}{psize}})) \tag{13}$$

By putting $RNF = 4 \times 10^{-14} W$, $P_i = 0W$ and $BW = 2 \times R$ into Eq(13), we get $P_{r\min} = 2.4 \times 10^{-13} W$. When estimating r_c, we usually leave fade margin because of small-scale fading. Fade margin is set between 20dB to 30dB. In our analysis, we use 30dB as a conservative value. So r_c can be estimated by solving the following equation.

$$P_r = P_t \times (\frac{\lambda}{4\pi})^2 \frac{1}{r_c^3} \frac{1}{10^3} \tag{14}$$

Replacing P_t, P_r and λ with $0.1W$, $2.4 \times 10^{-13} W$ and $0.125m$, we get $r_c = 35m$. We are not asserting that two nodes with distance bigger than r_c will not be able to establish a

data link. But r_c is a relatively conservative range that nodes can safely communicate with each other by an acceptable PER considering the impact of both the large-scale path loss and small-scale fading. When we evaluate the average P_r at a certain distance, we do not have to add the fade margin because small-scale fading can cancel each other in average P_r. In order to constrain our computation within the area we are most interested with, we only consider the situation where the receiver and the eavesdropper are within r_c when we analyze the performance of CJWN scheme.

Another very important model of our analysis is the node distribution model. For an ad hoc network, it is good to assume that nodes are Poisson-distributed with δ being the node density. Without losing generality, we assume $\delta = 0.1 node/m^2$.

Mechanism of CJWN Scheme

The Figure 8 gives us the top view of the layout for the CJWN scheme.

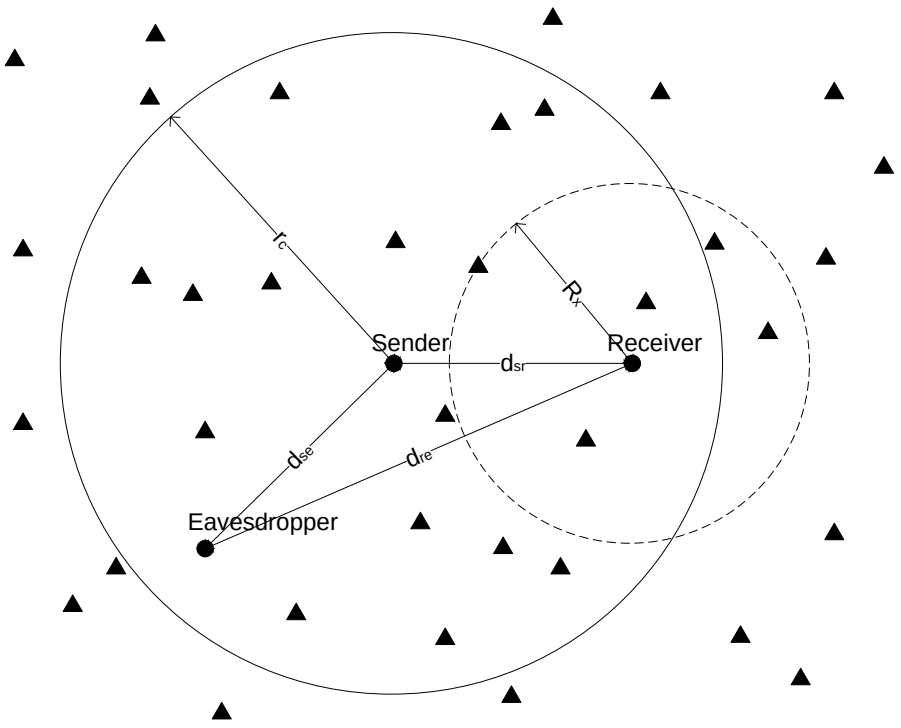

Figure 8 Layout of CJWN

The receiver and the eavesdropper are randomly located within the communication range of the sender. All the other triangles indicate other cooperative nodes that will help the sender and the receiver in CJWN. In Figure 8, the distance R_x is the range to divide all the cooperative nodes into two parts. Those nodes within R_x will keep silence during the transmission of DATA packets from the sender to the receiver, and those nodes out of R_x will all emit noise at the power of P_{noise}. Roughly, we can regard the neighborhood of the receiver within R_x as a "vacuum" region. It is easy to prove that the accumulated power of noise from cooperative nodes will reach a minimum value at the receiver's position. Respectively, d_{sr}, d_{se} and d_{re} stand for the distances between the sender and the receiver, between the sender and the eavesdropper, and between the receiver and the eavesdropper.

In the time domain, the Figure 9 shows the simple operation of CJWN scheme.

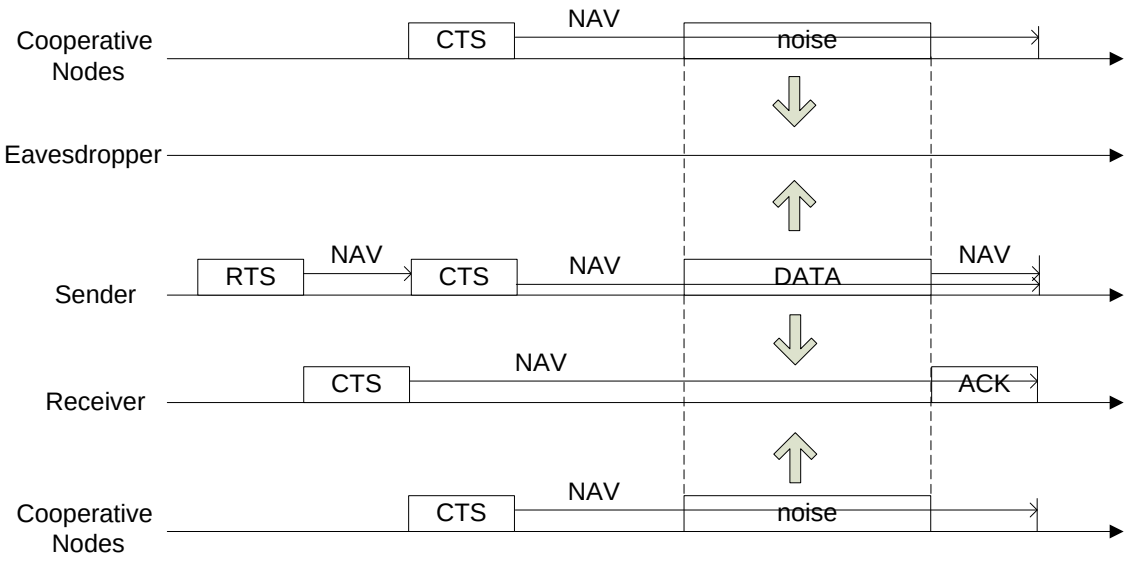

Figure 9 Time Domain Operation of CJWN

The entire process of CJWN scheme can be described as the following steps.

- ✧ When the sender wants to use CJWN scheme to send a secret DATA packet to the receiver, the RTS packet will contain a flag telling the receiver that the

coming DATA packet will be protected by CJWN scheme. The duration information attached in this RTS packet only extends NAV to the end of the CTS from the receiver.

- ✧ Receiving the RTS packet, the receiver broadcasts CTS packet to all the nodes in the network including the sender. The duration attached in this CTS packet will extend the NAV to the end of ACK packet. Moreover, the receiver will calculate T_{DATA}, and contain it in the CTS packet. Other important parameters to be attached are the R_x and P_{noise}.
- ✧ On hearing the CTS packet, nodes deduct T_{DATA} and T_{ACK} from duration information, and update NAV. If the remaining is less than T_{CTS}, they will not relay this CTS packet any more. Otherwise, they will update the duration by deducting T_{CTS} from it, and broadcast it at once.
- ✧ From the received CTS packets, the sender will know the time to start the DATA packet, and other cooperative nodes will start the noise signal at the same time. Once exception is that the nodes within R_x will only take part in the broadcasting, and will not emit the noise.
- ✧ After receiving the DATA packet successfully, the receiver will reply with an ACK packet.

During the steps above, there are two questions left unanswered.

- ➢ How can the receiver determine R_x and P_{noise} attached?
- ➢ How can the cooperative nodes know whether they are within R_x or not?

Given the node density δ, R_x and P_{noise} are the key factors that affect the PER at the receiver. The receiver must ensure that R_x and P_{noise} will not make its PER higher than the maximum acceptable value of 5%. P_r is already known when the receiver hears

RTS packet from the sender, and RNF is determined by the hardware. According to Equation (11) and (12), we can determine the maximum acceptable P_i, $P_{i\max}$ with Eq(15).

$$P_{i\max} = \frac{-BW \times P_r}{R \times \ln(2 \times (1-(1-PER_{\max})^{\frac{1}{psize}}))} - RNF \tag{15}$$

At the same time, the P_i can be calculated by R_x and P_{noise} with Eq(16).

$$\begin{aligned} P_i &= \int_{R_x}^{+\infty} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr \\ &= \frac{\delta P_{noise} \lambda^2}{8\pi R_x} \end{aligned} \tag{16}$$

Combining (15) and (16) we get the constraint of $\frac{P_{noise}}{R_x}$.

$$\frac{P_{noise}}{R_x} \le \frac{8\pi}{\delta\lambda^2} \times \left(\frac{-BW \times P_r}{R \times \ln(2 \times (1-(1-PER_{\max})^{\frac{1}{psize}}))} - RNF\right) \tag{17}$$

With a fixed R_x we expect P_{noise} to be as large as possible, which can achieve a higher P_i at the eavesdropper. So we turn the inequality into equality. The exception is P_{noise} can't be larger than P_t (100mW in our case). In order to make the eavesdropper suffer from a maximum P_i, we can come up with a best pair of R_x and P_{noise}. The next section will explain the best pair in detail.

There are some ways to measure the distance between nodes. One easy but costly way is to equip each node with a GPS system. In our scheme there is another cheaper one. The performance evaluation of CJWN in the next section will show that the best R_x always appears within r_c. It means that those cooperative nodes keeping silence are always in the

communication range of the receiver. Those nodes who can't hear the receiver's CTS packet will always emit noise. Those who can hear must compare the power of the CTS packet with $P_t \times \frac{\lambda^2}{(4\pi)^2 R_x^3}$ to determine their positions.

CJWN Performance Analysis

The performance of CJWN scheme can be evaluated by the eavesdropper's PER. The only assumption we make on the eavesdropper is that it is in the communication range of the sender. As stated in the previous section, the R_x and P_{noise} are constrained by Eq(17), which ensures the receiver's PER is always acceptable.

We denote the eavesdropper's P_r and P_i as P_{er} and P_{ei}. P_{er} is calculated as a function of d_{se}.

$$P_{er} = \begin{cases} \frac{P_t \lambda^2}{(4\pi)^2 d_{se}^3} & \text{if } d_f \le d_{se} \le r_c \\ \frac{P_t \lambda^2}{(4\pi)^2 d_f^3} & \text{if } d_{se} < d_f \end{cases} \tag{18}$$

P_{ei} is calculated as a function of d_{re}. It is a bit more complicated than P_{er}.

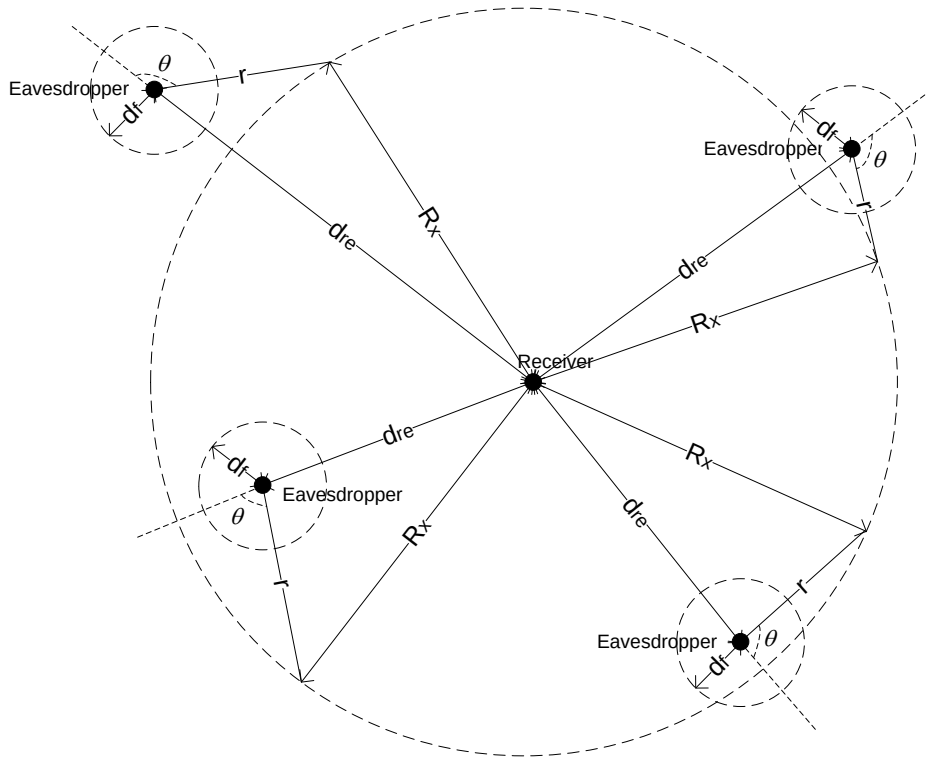

Figure 10 Calculation of P_{ei}

In Figure 10 we divide the P_{ei} into four regions, which are ($0 < d_{re} \le R_x - d_f$), ($R_x - d_f < d_{re} \le R_x$), ($R_x < d_{re} \le R_x + d_f$) and ($R_x + d_f < d_{re}$). The θ is equal to $\arccos(\frac{R_x^2 - r^2 - d_{re}^2}{2rd_{re}})$.

✧ $0 < d_{re} \le R_x - d_f$ (19)

$$P_{ei} = \int_{R_x - d_{re}}^{R_x + d_{re}} \frac{\theta}{\pi} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr + \int_{R_x + d_{re}}^{+\infty} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr$$

$$= \int_{R_x - d_{re}}^{R_x + d_{re}} \frac{\theta \delta P_{noise} \lambda^2}{8\pi^2 r^2} dr + \frac{\delta P_{noise} \lambda^2}{8\pi (R_x + d_{re})}$$

✧ $R_x - d_f < d_{re} \le R_x$ (20)

$$P_{ei} = \int_{d_f}^{R_x+d_{re}} \frac{\theta}{\pi} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr + \int_{R_x+d_{re}}^{+\infty} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr$$

$$= \int_{d_f}^{R_x+d_{re}} \frac{\theta \delta P_{noise} \lambda^2}{8\pi^2 r^2} dr + \frac{\delta P_{noise} \lambda^2}{8\pi(R_x + d_{re})}$$

✧ $R_x < d_{re} \le R_x + d_f$ (21)

$$P_{ei} = \pi(d_{re} - R_x)^2 \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 d_f^3} + \int_{d_{re}-R_x}^{d_f} \frac{\theta}{\pi} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 d_f^3} dr$$

$$+ \int_{d_f}^{R_x+d_{re}} \frac{\theta}{\pi} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr + \int_{R_x+d_{re}}^{+\infty} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr$$

$$= (d_{re} - R_x)^2 \frac{\delta P_{noise} \lambda^2}{16\pi d_f^3} + \int_{d_{re}-R_x}^{d_f} \frac{\theta r \delta P_{noise} \lambda^2}{8\pi^2 d_f^3} dr$$

$$+ \int_{d_f}^{R_x+d_{re}} \frac{\theta \delta P_{noise} \lambda^2}{8\pi^2 r^2} dr + \frac{\delta P_{noise} \lambda^2}{8\pi(R_x + d_{re})}$$

✧ $R_x + d_f < d_{re}$ (22)

$$P_{ei} = \pi d_f^2 \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 d_f^3} + \int_{d_f}^{d_{re}-R_x} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr$$

$$+ \int_{d_{re}-R_x}^{R_x+d_{re}} \frac{\theta}{\pi} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr + \int_{R_x+d_{re}}^{+\infty} 2\pi r \delta P_{noise} \frac{\lambda^2}{(4\pi)^2 r^3} dr$$

$$= \frac{\delta P_{noise} \lambda^2}{16\pi d_f} + \int_{d_f}^{d_{re}-R_x} \frac{\delta P_{noise} \lambda^2}{8\pi r^2} dr$$

$$+ \int_{d_{re}-R_x}^{d_{re}+R_x} \frac{\delta P_{noise} \theta \lambda^2}{8\pi^2 r^2} dr + \frac{\delta P_{noise} \lambda^2}{8\pi(R_x + d_{re})}$$

Here we provide a simple example to show the effect of CJWN scheme on the eavesdropper's PER. In this example, d_{sr} is 20m and R_x is 8m. According to Eq(17), we can get the maximum acceptable $P_{noise} = 2.63 \times 10^{-5} W$. Eq(18) can give us P_{er} in the communication range, which is shown in Figure 11. The sender is located at (0, 0) and the receiver is located at (20, 0). Since the eavesdropper is in the communication range, it can hear the packets from the sender clearly without CJWN enable.

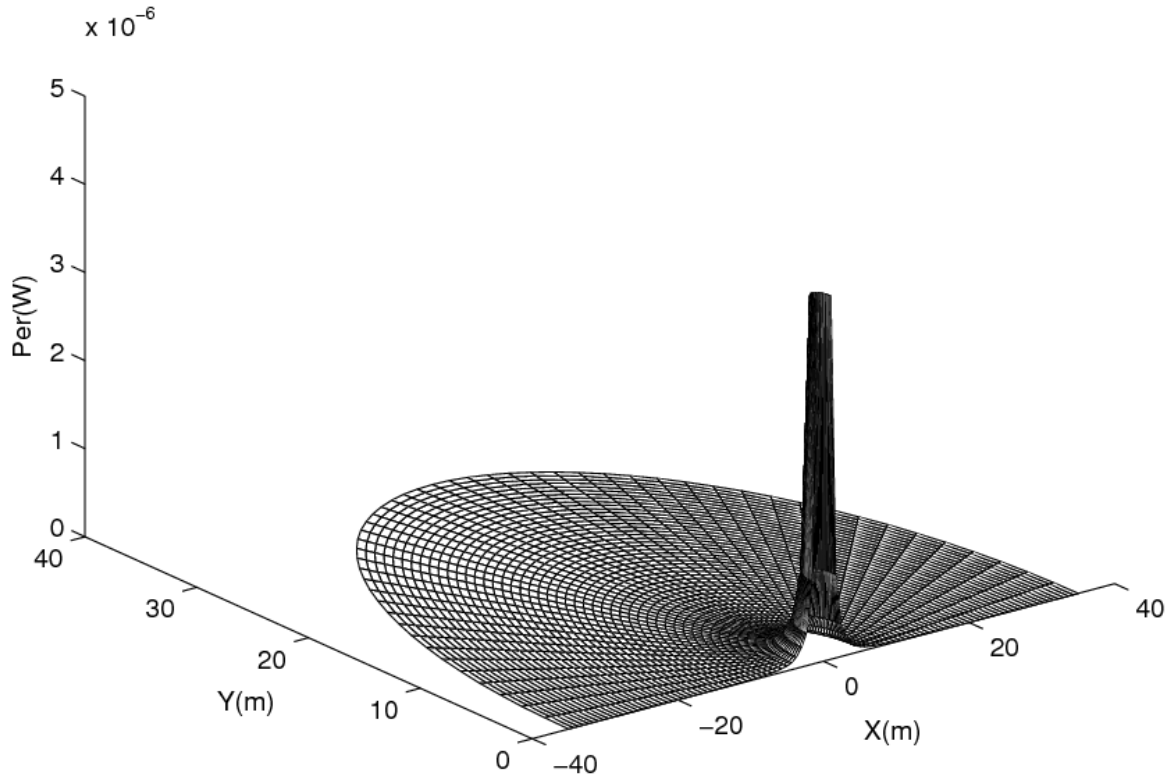

Figure 11 P_{er} within r_c

Equation (19), (20), (21) and (22) can give us P_{ei} in the communication range, which is shown in Figure 12.

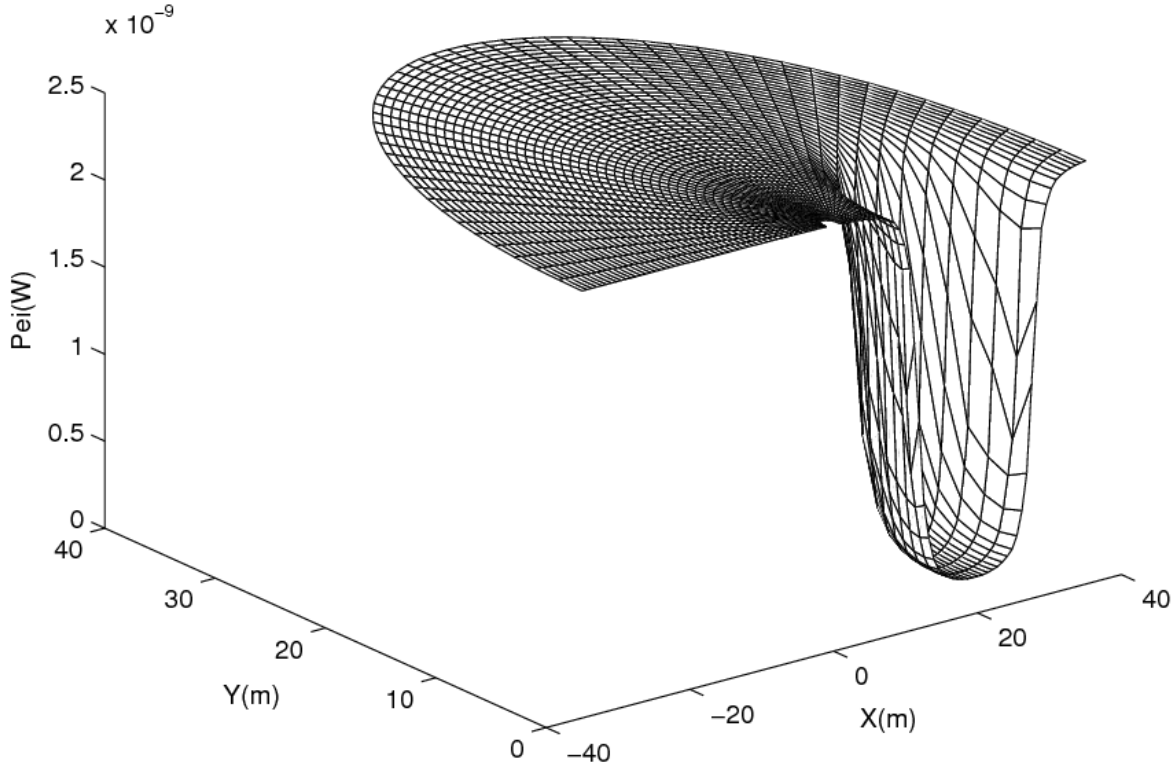

Figure 12 P_{ei} within r_c

After getting P_{er} and P_{ei}, we can further calculate the PER at the eavesdropper with the help of Eq(11) and (12). The result is also plotted in Figure 13.

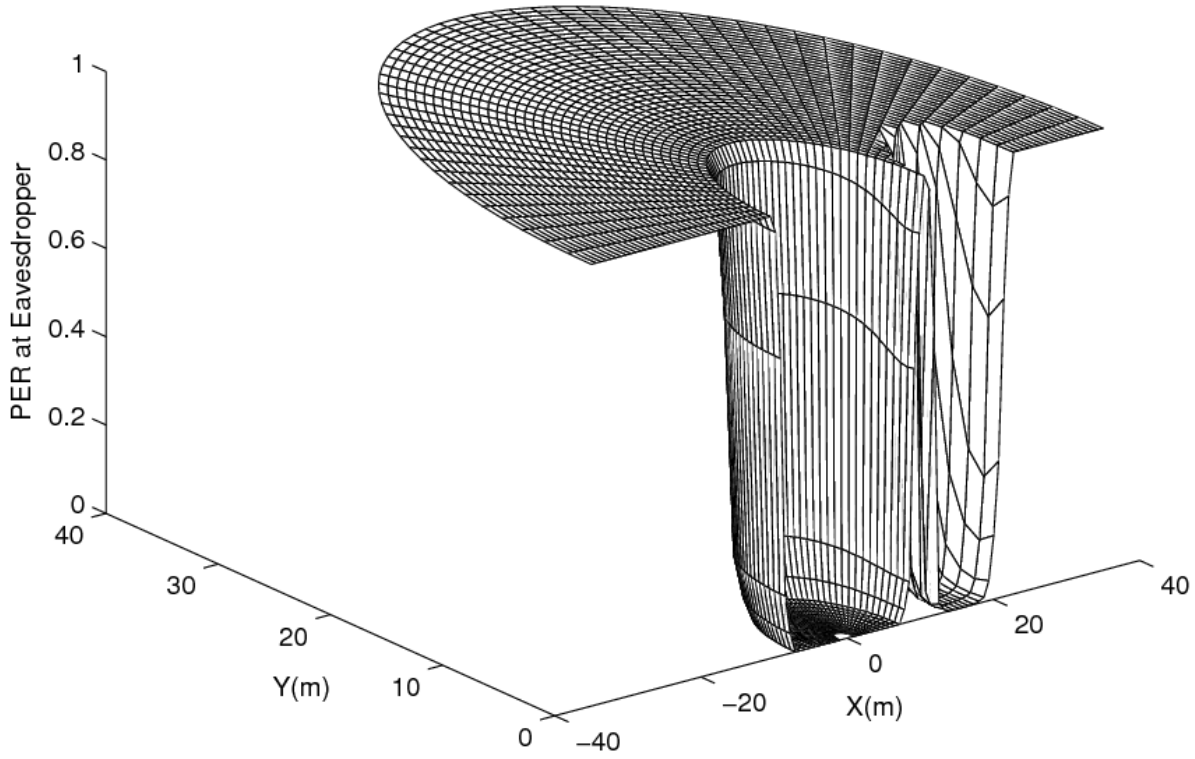

Figure 13 PER of Eavesdropper

We can see that, except the regions close to the sender and the receiver, most part of the communication range can no longer provide an acceptable PER to the eavesdropper, which will increase the security of the DATA packet.

In order to achieve a best protection effect, we are trying to find out the most optimal pair of R_x and P_{noise} with a specified d_{sr}. We use the expected value of PER at the eavesdropper as the optimizing target.

$$E(PER) = \int_0^{2\pi} \int_0^{r_c} \frac{d_{se} PER(\theta, d_{se})}{\pi r_c^2} dd_{se} d\theta \tag{23}$$

The θ is the angle at the sender formed by the sender, the receiver and the eavesdropper. For each d_{sr}, the choice of the pair of R_x and P_{noise} will affect the resulting E(PER). We can use Eq(23) to establish a mapping between the R_x and the E(PER). Several values of d_{sr} are selected to show the mapping in Figure 14.

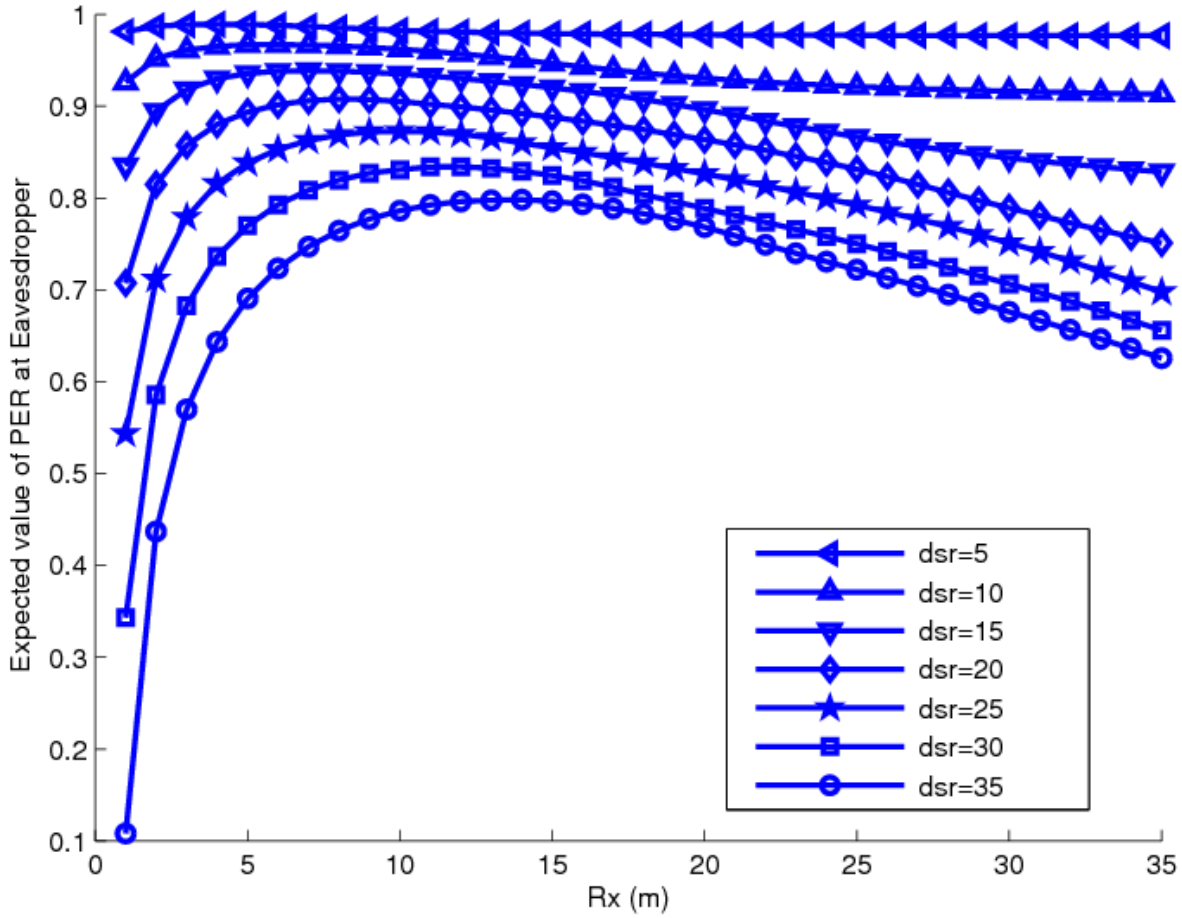

Figure 14 Mapping between R_x and E(PER)

Obviously, no matter what d_{sr} is, the best R_x for a maximum E(PER) is within the communication range, and E(PER) can be increased to at least 80% by CJWN. Without CJWN scheme, the PER of eavesdropper in the transmission range r_c is definitely less than 5%.

According to our research, it is hard to theoretically derive an expression of the best R_x. So it is suggested to use a table to store the pre-calculated R_x and P_{noise} pair according to different node density δ and d_{sr}.

A Practical Approach of CJWN Scheme

As we have discussed in the previous section, the CJWN relies on R_x and P_{noise} pair to perform the DATA packet protection. There are several practical problems with that.

First, because of the existing of the small-scale fading, pre-calculated R_x and P_{noise} pair can hardly fit with various environments. Second, R_x and P_{noise} pair is picked based on node density and d_{sr}, the distance between the sender and the receiver. d_{sr} is calculated with large-scale fading, and it may not be accurate enough when there is strong small-scale fading existing.

So we suggest a more practical and accurate approach of CJWN scheme. As we have observed from the Figure 14, no matter what the d_{sr} is, the best R_x is always about 10m. Based on this fact, we will always fix R_x at 10m. Here are the basic steps we will need to carry out.

- ✧ Before we can actually run CJWN in a specified ad hoc network, we will need to calibrate with the nodes who will be the receivers in the CJWN. The calibrating node will first broadcast a packet called Request To Calibrate (RTC). In this packet there contains three parameters.
  - (1) First one is the time to start the whole calibration process, T_{start}.
  - (2) Second one is the threshold of received power P_{sh} calculated by

$$P_{sh} = P_t \times (\frac{\lambda}{4\pi})^2 \frac{1}{R_x^3} \quad (24)$$

  - (3) Third one is the array of P_{noise} to be calibrated. If there are totally N values of P_{noise}, we can mark them as:

$$P_{noise}[0],\ P_{noise}[1],\ P_{noise}[2],\ \ldots,\ P_{noise}[N-1]$$

- ✧ Up on hearing the RTC packet, all the other nodes will broadcast it until T_{start} is reached.

- When the calibration starts, there are two groups of nodes that will behave differently. Some of them receive the calibrator's RTC packet directly and the received power is less than P_{sh}. Then they will keep silence during the calibration. Other nodes will send out noise at the power assigned by the P_{noise} array.
- The calibrator will listen to the accumulated power levels ($P_i[0], P_i[1], P_i[2]$, …, $P_i[N-1]$) of incoming noise and record them. In the memory there will be a calibration chart as Figure 15.

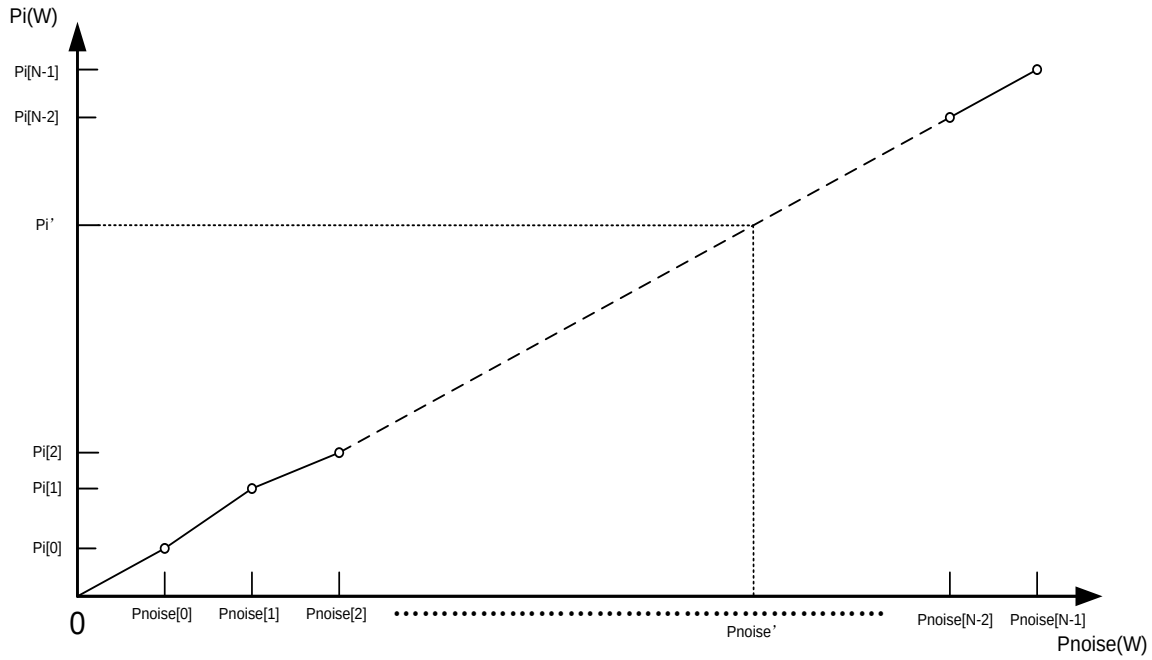

Figure 15 Calibration char

- When the actual data transmission happens, the sender sends RTS packet to the receiver. One important thing the receiver needs to do is to measure the received power of the RTS packet, P_r. It is reasonable to assume that the received power of DATA packet will be the same as P_r. Then the receiver can calculate the required accumulated noise power level, P_i'.

$$P_i' = \frac{-BW \times P_r}{R \times \ln(2 \times (1 - (1 - PER_{\max})^{\frac{1}{psize}}))} - RNF \quad (25)$$

- ✧ With the help of calibration char and P_i', the receiver can find the corresponding P_{noise}. Then it can attach the duration information, the threshold of received power P_{sh} and the required noise power level, P_{noise}'. The prepared CTS packet will be broadcasted.
- ✧ When a node hears the CTS packet, it will first deduct duration value by T_{CTS}. If the remaining is less than $T_{DATA} + T_{ACK}$, it will not broadcast CTS packet again. Otherwise, it will update the duration value in the CTS packet with the remaining and broadcast it again.
- ✧ When the DATA packet starts transmission, two groups of the cooperative nodes will have different behaviors. It is actually the same with the calibration procedure. Some nodes heard the CTS packet from the receiver directly and the received power of CTS packet is less than P_{sh}, and they will keep silence. Other cooperative nodes will send out noise at the power level of P_{noise}', which is attached in the CTS packet. What we are expecting is the accumulated noise power level at the receiver will be very close to P_i', and the resulting PER of the receiver will be acceptable.
- ✧ When the receiver has successfully received the DATA packet, it will certainly reply with an ACK packet.

This practical approach of CJWN no longer relies on the theoretical calculation from R_x to P_{noise}. It only relies on the actually data gathered from the calibration procedure. The calibration data can characterize the actual propagation property of the surrounding environment. If the wireless nodes are casted by plane into the battle field, they are

relatively static to each other. Once the calibration is finished, it is reasonable to believe that the nodes do not have to re-calibrate for a long time.

The theoretical background of the calibration needs a bit more explanation. After the nodes are broadcasted, they are not likely to move. So the wireless channels between the receiver and any other nodes are usually regarded as Linear and Time Invariable (LTI) system. So the increase in the P_{noise} will cause the proportional increase in the accumulated received power of noise at the receiver. Theoretically the calibration chart should have a straight line without any change in the channel status. But practically there are always some factors making the channels unlinear. This is why we set many check points in the calibration chart.

In order to verify the effectiveness of our scheme, I did the simulation with the OMNeT++[20], ChSim[21] and Matlab[22]. First a simulation scene is generated randomly.

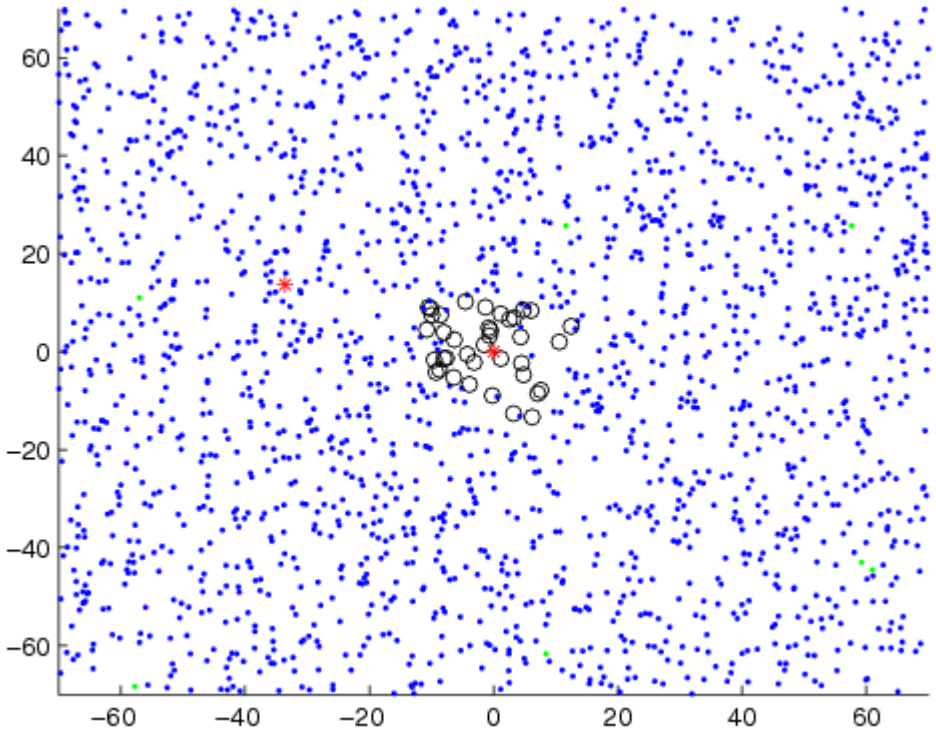

Figure 16 Randomized Simulation Scene

This is scene has the node density of $0.1/m^2$. The red star in the center is the designated receiver, and the other red start is a randomly chosen sender. Of course the

power of the signal from the sender at the receiver is strong enough for a PER bigger than 5%. The black circles stand for the cooperative nodes whose received power of CTS packet is bigger than P_{sh}. As designed, those nodes will not emit noise when the DATA packet is transferred. All the remaining nodes will help the sender and the receiver by emitting noise at the power of P_{noise} to protect the DATA packet. Notice there are blue dots and green dots. The blue ones can hear the CTS directly but the green ones require multiple hops from the receiver. In the Figure 16, the distances from the black circles to the receiver do not have a cutting edge of $R_x = 10m$. Some are bigger and some are smaller. The reason is that we have put the small-scale fading into the channels, which causes the fluctuations.

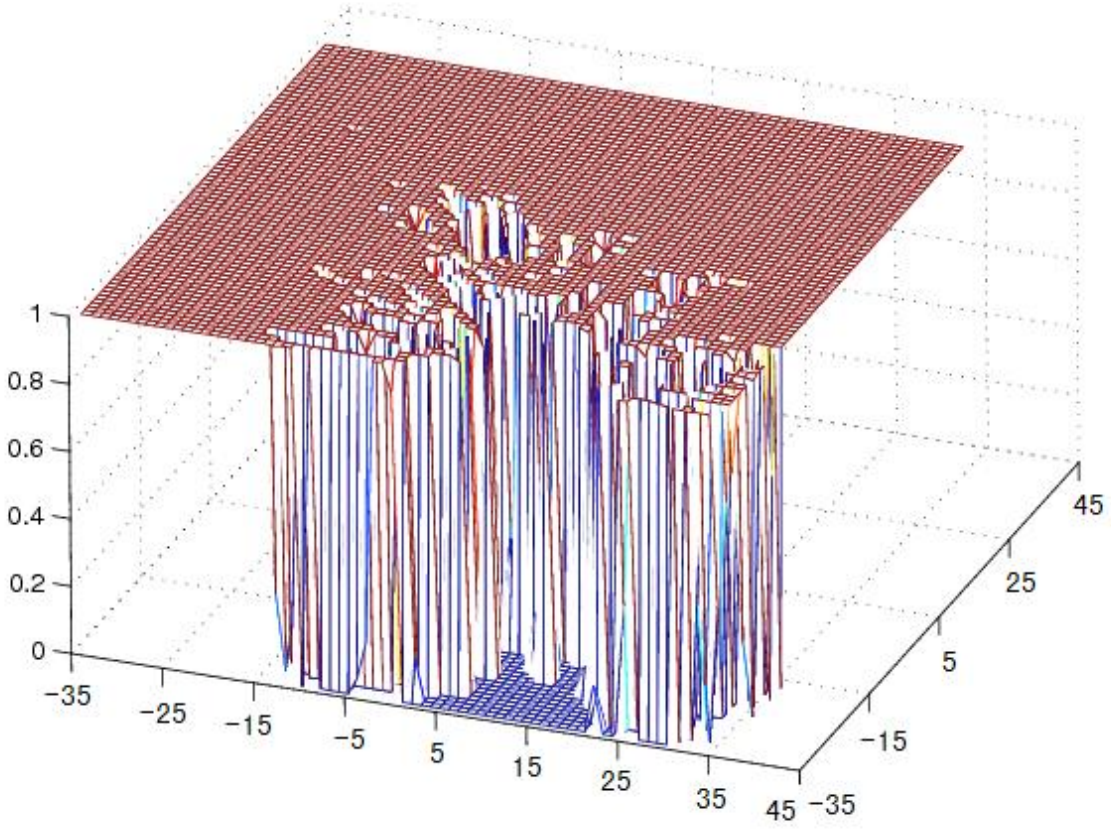

Figure 17 Packet Error Rate at Eavesdroppers

Figure 17 shows the final packet error rates at the eavesdroppers within the 70m by 70m area around the receiver. From the Figure 16 we can see that most of the eavesdroppers can have a clear signal from the sender if there is no CJWN scheme applied. With the CJWN in Figure 17 we can see that most of that area is no longer suitable for

eavesdroppers since the packet error rate is increased to almost 100%. Only the area close to the sender or the receiver is not protected by the noise from our cooperative nodes.

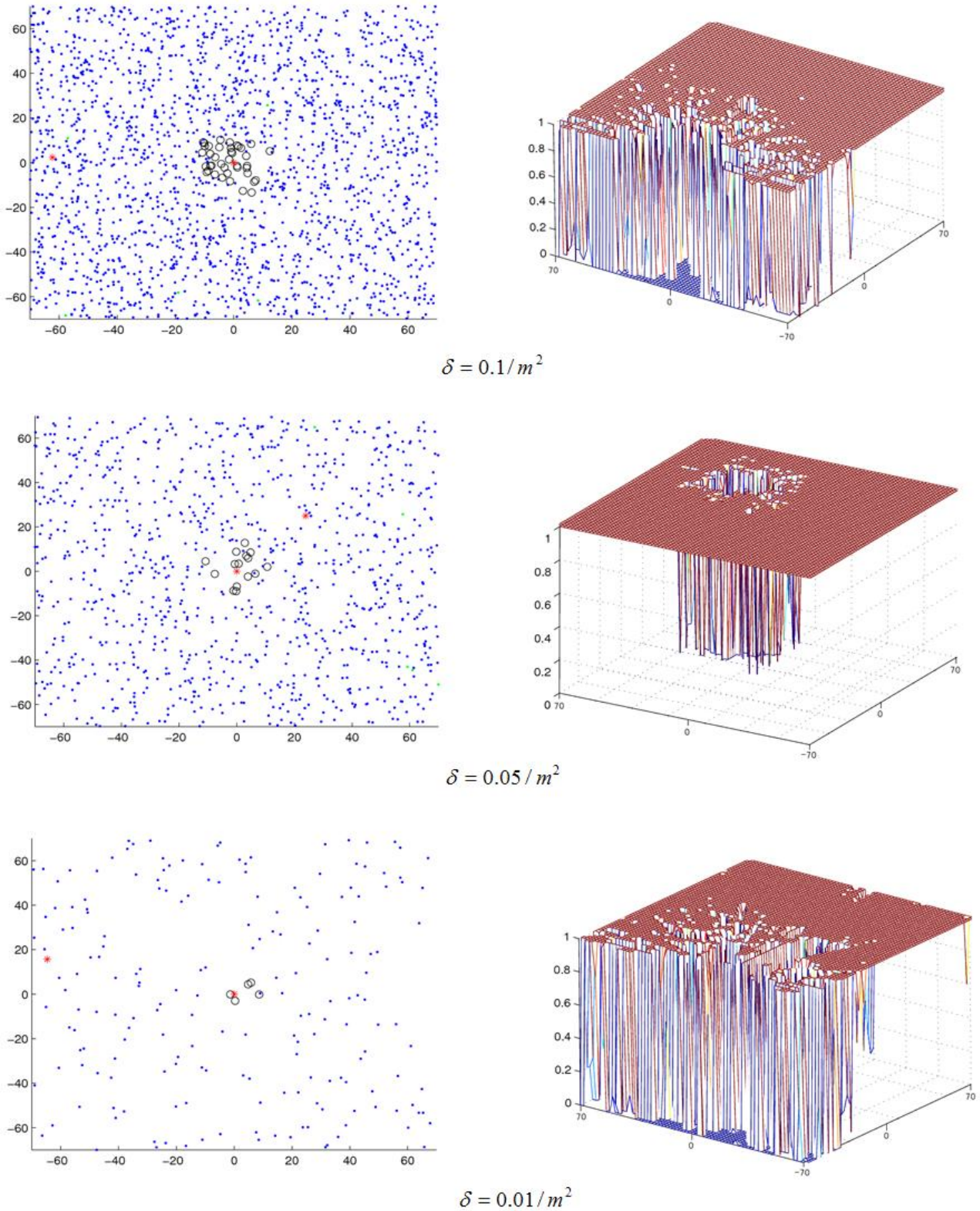

Figure 18 Effects of CJWN in Scenes of Different Node Density

Also I did multiple simulations on the effects of the CJWN scheme in the scenes of different node density (δ). Figure 18 shows the simulation results of $\delta = 0.1/m^2$, $\delta = 0.05/m^2$ and $\delta = 0.01/m^2$. All the three cases prove that the CJWN scheme can cover most of the neighborhood.

Conclusion and Future Work

In the field of wireless communication, the attacking and defending mechanisms are always evolving. There is no panacea to solve every security problem for wireless networks. Eavesdropping has long been a big problem in wireless communication. People have developed many schemes to fight against it, such as different encryption/decryption schemes in cryptography. But some time people may have to send very important message in plain text, like the key distribution. According to such kind of requirement, we have developed the CJWN scheme to protect the DATA packet with the help from cooperative nodes in the ad hoc networks.

Normally, jamming is an attacking method to destroy the message receipt of the receiver. CJWN is actually making use of the jamming to protect our message from being sniffed. Our evaluation of CJWN's performance has shown that it can effectively increase the PER of the eavesdropper in the sender's communication range, especially at the far end of the ender and the receiver. Allied with other security schemes, such as encryption/decryption schemes, CJWN can further decrease the risk of information exposure. In order to turn CJWN into a more useful and practical scheme, we come up with a more realistic approach of CJWN.

However there are some constraints in CJWN scheme. First, it can hardly prevent the DATA packet from being heard by eavesdropper which is very close to the sender or the receiver. Second, it is very obvious that CJWN costs much more time and energy resource than the normal CSMA/CA scheme. So whether to use it depends on how secret the information is.

The future work related with CJWN scheme may include the following question. In the real world, we can't require all the cooperative nodes to help in CJWN. It is because the broadcasted CTS packet has its reaching area. How big the area is depends on the node density δ and the hops of CTS packet. In our analysis of the performance, we make the area infinite. Further research work can be done on the searching for the reliable hop number with specific δ.

References

[1] T. Rappaport: *Wireless Communications Principles and Practice (2nd Edition)*, Prentice Hall, Jan 10, 2002

[2] David Tse and Pramod Viswanath: *Fundamentals of Wireless Communication*, Cambridge University Press, 2005

[3] *Wireless Security*, http://en.wikipedia.org/wiki/Wireless_security

[4] C. Siva Ram Murthy and B.S. Manoj: *Ad Hoc Wireless Networks: Architectures and Protocols*, Prentice Hall, Jun 3, 2004

[5] E. Shi and A. Perrig: *Designing secure sensor networks*, Carnegie Mellon University, December 2004

[6] H. Chan and A. Perrig: *Security and privacy in sensor networks*, Carnegie Mellon University, October 2003

[7] S. Board: *Std 802.11 part 11 Wireless LAN medium access control (MAC) and physical layer (PHY) specifications*, June 2003

[8] T. N. R. R. Amit Sinha, Issam Haddad and D. Thomas: *Wireless intrusion protection system using distributed collaborative intelligence*, 2006 IEEE International Performance Computing and Communications Conference, April 2006

[9] *Effetch*, http://www.effetech.com/

[10] *WEPCrack*, http://sourceforge.net/projects/wepcrack/

[11] *AirSnort*, http://airsnort.shmoo.com

[12] *NsNam*, http://www.isi.edu/nsnam/ns/

[13] Kyunghan Lee, Bang Chul Jung, Injong Rhee, Song Chong and Dan Keun Sung: *Revisiting the Transmission Range Model in Mobile Networks based on IEEE 802.11a/g*, IEEE Communications Letters, March 2008

[14] Thorsten Pawlak and Stefan Valentin: *ChSim-A wireless channel simulator for OMNeT++*, University Paderborn, September 2006

[15] David Tse and Pramod Viswanath: *Fundamentals of Wireless Communication*, Cambridge University Press, June 2005

[16] James K. Cavers: *Mobile Channel Characteristics*, Kluwer Academic Publishers, 2000

[17] Emma Carlson, Martin Kubisch and Daniel Hollos: *A Receiver Based Protecting Protocol for Wireless Multi-hop Networks*, International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems, 2005

[18] Jim Zyren and Al Petrick: *Tutorial on Basic Link Budget Analysis*, Intersil Corporation, June 1998

[19] *Product Datasheet of Wireless USB 2.0 Adapter SUB-3701*, Engenius Technologies Singapore Pte Ltd, April 2006

[20] *OMNeT++,* http://www.omnetpp.org/

[21] *ChSim*,http://www.cs.uni-paderborn.de/en/fachgebiete/research-group-computer-networks/projects/chsim.html

[22] *MATLAB*, http://www.mathworks.com/

Vita

Jingqi Wu was born in Ningbo, Zhejiang China. He received his B.S. in Electrical Engineering and his M.S. in Mechanical Engineer from Zhejiang University (China). After coming to U.S he pursued his M.S. in Computer Science from University of New Orleans.