Important characteristics of the wigig technology computer science

Wireless Gigabit is an up-and-coming technology expected to enable wireless connectivity of up to 7Gbps in data, display and audio applications. The organization sponsoring this technology is the Wireless Gigabit Alliance.

Features of Wigig:

Some of the important characteristics of the Wigig technology are listed below:

Wigig is capable of providing a wireless network which its speed is up to 7Gbps, while the fastest current 802. 11n has theoretically the highest speeds up to 600Mbps.

WiGig is operated at 60GHz which allows a wider channel and supports super-fast transfer speeds. It can transfer data between 1Gbps to 7Gbps, 60 times more than Wi-Fi.

Wigig can be able to support the Tri band devices.

WiGig is a multi-gigabit communication technology which is an ideal standard for the use of streaming HD video so it can display full 1080 pixels of the PC to the TV via a wireless network.

How does Wigig works:

Wigig will primarily be used within a single room to provide wireless connectivity between home entertainment equipment. It will enable very fast data transfers and streaming media which is 10 times faster than the old wireless technologies, in addition to wireless connections for cameras, laptops.

DeliverablesTechnical Issues

Current and future expectations of WiGig deployment.

Types of challenges or difficulties are there related to WiGig implementations.

Kinds of organisations might need these new standards.

Security Issues

Discuss and analyse the security issues that might arise due to wide deployment of WiGig Alliance. (802. 11 security issue and the Galois/Counter Mode of the AES encryption algorithm)

Discuss and analyse cross layer security framework in Wireless LAN deployment. Is that framework will improve security in WLAN or not.

Technical IssuesCurrent Wigig deployment

The industry standard relevant to Wigig is IEEE 802. 11ad. Draft 1. 0 of the specification was published in Jan 2011. Per the draft standard, signals will occupy the unlicensed 60 GHZ frequency band and all 802. 11 ad-compliant devices will provide backward compatibility with 802. 11 standard. As a result, tri-band devices will operate at 2. 4, 5. 0 and 60 GHz.

The Wigig specification includes main features to maximize performance, minimize implementation complexity and cost, enable backward compatibility with existing Wi-Fi and provide advanced security. Key features include:

Support for data transmission rates up to 7 Gbps.

Wigig operates at 60 GHz band that means it has much more spectrum available, the channels are much wider, enabling multi-gigabit data rates. Wigig defines 4 channels, each 2. 16 GHz wide which is 50 times wider than the channels available in 802. 11n.

Seamless switching between 2. 4/5/60 GHz bands

Based on IEEE 802. 11, Wigig provides native Wi-Fi support and enables devices which has tri-band radios to be able to transparently switch between 802. 11 network operating in any frequency band including 2. 4/5/60 GHz

Support for beamforming, a technology which maximize the signal strength and enable robust communication at distances beyond 10 meters.

WiGig is integrated a technology, called “ Beamforming”. It allows the radio beam is shot to the right target with the best performance; minimize waste in the process of transmission. Thus, WiGig uses energy more efficient than traditional Wi-Fi connection.

Beamforming employs directional antennas to reduce interference and focus the signal between two devices into a concentrated “ beam”. This allows faster data transmission over longer distances.

Beamforming is defined within the PHY and MAC layers.

During the beamforming process, two devices establish communication and then fine-tune their antenna settings to improve the quality of directional

communication until there is enough capacity for the desired data transmission.

The devices can quickly establish a new communications pathway using beams that reflect off walls when an obstacle blocks the line of sight between two devices or if someone walks between them.

http://genk2. vcmedia. vn/N0WoyYblO3QdmZFKPMtKnadHAHTevz/Image/2012/04/2_6a565. jpg

Advanced security using the Galois/Counter Mode of the AES encryption algorithm.

AES-GCM is an authenticated encryption algorithm designed to provide both authentication and privacy. Developed by David A McGrew and John Viega, it uses universal hashing over a binary Galois field to provide authenticated encryption.

GCM was designed originally as a way of supporting very high data rates, since it can take advantage of pipelining and parallel processing techniques to bypass the normal limits imposed by feedback MAC algorithms. This allows authenticated encryption at data rates of many ten of Gbps, permitting high grade encryption and authentication on system which previously could not be fully protected.

Different types of layers take part in the working of the wireless gigabit technology, physical layer (PHY) deals with all the devices of low and high power and maintain the status of communication.

Protocol adaption layers (PALs) are being developed to support specific system interfaces including data buses for PC peripherals and display interfaces for HDTVs, monitors and projectors.

Supplements and extends the 802. 11 Medium Access Control(MAC) layer and is backward compatible with the IEEE 80211 standard

Power Management

Wigig devices can take advantage of a new scheduled access mode to reduce power consumption. Two devices communicating with each other via a directional link may schedule the periods during which they communicate; in between those periods, they can sleep to save power.

802. 11 ad draft standard is compared to other wireless technology

http://images-news. easyvn. net/upload/2011/12/08/article/cong-nghe-khong-day-60-ghz-cho-docking-usb-hdmi_3. jpg

Wigig in future

WGA has announced the launch of a new wireless connection standard, Wigig 1. 1 ready for certification. The Wigig 1. 1 is added 2 new PALs specifications, the Wigig Display Extension (WDE) and Wigig Serial Extension (WSE) to supplement the previously published Wigig Bus Extension (WBE) and MAC/PHY specifications.

Structure of Wigig

Wigig is defined in 2 layers based on IEEE 802. 11. They are Physical and Medium Access Control layers. These layers enable native support for IP networking over 60Ghz band. They make simpler and less expensive to produce devices that can communicate over both Wigig and existing Wi-Fi using tri-band radios (2. 4GHz, 5GHz and 60 GHz).

http://farm3. static. flickr. com/2390/5791077356_c2146fb4f0. jpg

Physical Layer

The physical layer of the 802. 11 ad standardized 2 wireless data exchange techniques:

Orthogonal frequency-division multiplexing (OFDM)

Single carrier (SC)

The 802. 11ad divides the 60GHz band into four 2. 16 GHz wide channels. Data rates of up to 7 Gbits/s are possible using OFDM with different modulation schemes. A single channel version for low power operation is available and can deliver a speed up to 4. 6 Gbits/s. These wide channels enable WIgig to support applications that require extremely fast communication, such as uncompressed video transmission.

The PHY in 802. 11ad is split into Physical Layer Convergence Protocol (PLCP) and the Physical Medium Dependent (PMD) sub layers. The PLCP parses data units transmitted/received using various 802. 11 media access techniques. The PMD performs the data transmission/reception and modulation/demodulation directly accessing air under the guidance of the

PLCP. The 802. 11 ad MAC layer to great extend is affected by the nature of the media. For instance, it implements a relatively complex for the second layer fragmentation of PDUs.

Medium Access Control (MAC) layer

Wigig shares MAC layer with existing 802. 11 networks enables session switching between 802. 11 networks operating in the 2. 4 GHz, 5GHz and 60 GHz bands, resulting in uninterrupted wireless data communications. The 802. 11 ad MAC layer has been extended to include beamforming support and address the 60 GHz specific aspects of channel access, synchronization, association and authentication.

Protocol Adaption Layer (PALs)

PAL is a layer added to network transmissions to help adapt to older standards. It allows wireless implementations of key computer and consumer electronics interfaces over 60GHz Wigig networks. The version 1. 0 A/V and I/O protocol adaption layer (PAL) specifications have been developed to support specific system interfaces including extensions for PC peripherals and display interfaces for HDTVs, monitors and projectors.

The Wigig Bus Extension (WBE)

Define high-performance wireless implementations of widely used computer interfaces over 60GHz.

Enable multi-gigabit wireless connectivity between any two devices, such as connection to storage and other high-speed peripherals

The Wigig Display Extension (WDE)

Support wireless transmission of audio/visual data

Enable wireless DisplayPort and other display interfaces that include the High-bandwidth Digital Content Protection 2. 0 feature.

Offers key A/V applications, such as the transmission of lightly compressed or uncompressed video from a computer or digital camera to an HDTV, monitor or projector.

http://img84. imageshack. us/img84/2195/fig2m. jpg

Modulation & Coding Scheme (MCS)

The specification supports two types of modulation and coding schemes, which provide different benefits. Orthogonal frequency-division multiplexing (OFDM) supports communication over longer distances with greater delay spreads, providing more flexibility in handling obstacles and reflected signals. The single carrier, suited to lower applications, achieves a data rate up to 4. 6 Gbits/s, while OFDM enables 7 Gbits/s.

Usage Models

Wigig has a high compatibility and is used for many purposes.

Wigig can act as an alternative method which is used for replacing old connectivity standards such as: USB, DisplayPort, PCIe and HDMI. In addition, it is backward compatible with most devices which using 802. 11 connectivity in the 2. 4 GHz and 5 GHz bands. The main function of Wigig is

to connect home entertainment devices together – tablets, smartphones, PC, TV and more.

http://images-news. easyvn. net/upload/2011/12/08/article/cong-nghe-khong-day-60-ghz-cho-docking-usb-hdmi_2. jpg

Challenges or difficulties are there related to WiGig implementations.

The biggest technical challenge is that these networks will operate in much higher frequencies, around 60 GHz. The higher the frequency is, the greater the propagation loss over distance. Another challenge is 60 GHz radio are absorbed by wood, bricks, human body and particularly paint are far more opaque to 60 GHz waves. Thus, Wigig is most suitable for in-room applications.

Attenuation of various materials by frequency

Besides that, the beamforming of compliant equipment needs to be within line of sight of receiving devices in order to work well. Even a person stepping between two communicating devices can break the signal. With these weaknesses, they will prevent Wigig from being implemented popularly in the future. Moreover, most today devices only support 802. 11 a/g/n; it will take time to replace all these devices with new devices which support 802. 11ad standard.

Kinds of organisations might need these new standards

WiGig is a multi-gigabit communication technology which is an ideal standard for the use of streaming HD video so it can display full 1080 pixels

of the PC to the TV via a wireless network. In addition, its speed is up to 7 Gbps which is very useful for so many organizations such as:

Multimedia organization (newspapers, advertisement, movie)

Financial organization (Bank, office, tax)

Education organization (TAFE, university)

Medical organization (Hospital)

IT organization (Intel, Dell, Apple etc.)

Government

Military

Security Issues

Due to Wigig is based on IEEE 802. 11 standards; it has the same security issues with 802. 11 a/b/g/n.

Easy to access

Wireless LANs are easy to find. To enable clients to find them, networks must transmit Beacon frames with network parameters. The information needed to join a network is also the information needed to launch an attack on a network. Beacon frames a not processed by any privacy functions, which means that your 802. 11 network and its parameters are available for anybody with an 802. 11 card. Attackers with high-gain antennas can find

networks from nearby roads or buildings and may launch attacks without having physical access to your facility.

Solution: Enforce Strong Access Control

Ensuring that wireless networks are subject to strong access control can mitigate the risk of wireless network deployment. Networks should place access points outside of security perimeter devices such as firewalls, and administrators should consider using VPNs to provide access to the corporate network. Strong user authentication should be deployed, preferably using new products based on the IEEE 802. 1x standard. 802. 1x defines new frame types for user-based authentication and leverages existing enterprise user databases, such as RADIUS.

“ Rogue” Access Points

Easy access to wireless LANs is coupled with easy deployment. When combined, these two characteristics can cause headaches for network administrators and security officers. Any user can run to a nearby computer store, purchase an access point, and connect it to the corporate network without authorization. “ Rogue” access deployed by end users poses great security risks. End users are not security experts, and may not be aware of the risks posed by wireless LANs. Many deployments that have been logged and mapped by “ war drivers” do not have any security features enabled, and a significant fraction have no changes from the default configuration.

Solution: Regular Site Audits

Like any other network technology, wireless networks require vigilance on the part of security administrators. The obvious way to find unauthorized networks is to do the same thing that attackers do: use an antenna and look for them so that you find unauthorized networks before attackers exploit them. Physical site audits should be conducted as frequently as possible.

Unauthorized Use of Service

Several war drivers have published results indicating that a clear majority of access points are put in service with only minimal modifications to their default configuration. Unauthorized users may not necessarily obey your service provider’s terms of service, and it may only take one spammer to cause your ISP to revoke your connectivity.

Solution: Design and Audit for Strong Authentication

The obvious defence against unauthorized use is to prevent unauthorized users from accessing the network. Strong, cryptographically protected authentication is a precondition for authorization because access privileges are based on user identity. VPN solutions deployed to protect traffic in transit across the radio link provide strong authentication.

MAC Spoofing and Session Hijacking

802. 11 networks do not authenticate frames. Every frame has a source address, but there is no guarantee that the station sending the frame actually put the frame “ in the air.” Just as on traditional Ethernet networks, there is no protection against forgery of frame source addresses. Attackers can use spoofed frames to redirect traffic and corrupt ARP tables. At a much

simpler level, attackers can observe the MAC addresses of stations in use on the network and adopt those addresses for malicious transmissions.

Attackers can use spoofed frames in active attacks as well. In addition to hijacking sessions, attackers can exploit the lack of authentication of access points. Access points are identified by their broadcasts of Beacon frames. Any station which claims to be an access point and broadcasts the right service set identifier (SSID, also commonly called a network name) will appear to be part of an authorized network. Attackers can, however, easily pretend to be an access point because nothing in 802. 11 requires an access point to prove it really is an access point. At that point, the attacker could potentially steal credentials and use them to gain access to the network through a man-in-the-middle (MITM) attack.

Solution: Adopt Strong Protocols and Use Them

Using methods based on Transport Layer Security (TLS), access points will need to prove their identity before clients provide authentication credentials, and credentials are protected by strong cryptography for transmission over the air.

Session hijacking can be prevented only by using a strong cryptographic protocol such as IPsec.

Using strong VPN protocols which require the use of strong user authentication with 802. 1x.

Traffic Analysis and Eavesdropping

802. 11 provides no protection against attacks which passively observe traffic. The main risk is that 802. 11 does not provide a way to secure data in transit against eavesdropping. Frame headers are always “ in the clear” and are visible to anybody with a wireless network analyser.

Security against eavesdropping was supposed to be provided by Wired Equivalent Privacy (WEP). However, it protects only the initial association with the network and user data frames. Management and control frames are not encrypted or authenticated by WEP, leaving an attacker wide latitude to disrupt transmissions with spoofed frames.

Solution: Perform Risk Analysis

When addressing the threat of eavesdropping, the key decision is to balance the threat of using only WEP against the complexity of deploying a more proven solution.

If wireless LAN is being used for sensitive data, WEP may very well be insufficient for your needs. Strong cryptographic solutions like SSH, SSL, and IPsec were designed to transmit data securely over public channels and have proven resistant to attack over many years, and will almost certainly provide a higher level of security.

Key Problems with WEP

Repeat in key stream which allows easy decryption of data for a moderately sophisticated adversary.

Weak implementation of the RC4 algorithm leads to an efficient attack that allows key recovery

Subject to brute force attacks (Short Keys)

Easily compromised keys (Shared keys/No Key management)

Message modification is possible

No user authentication occurs

Subject to Man in the Middle attacks

WPABenefits

Improved Cryptography

Strong Network access control

Will Support 802. 1x, EAP, EAP-TLS, Radius, and Pre-Placed Keys

Key Management

Replay Protection

Provides for data and header integrity

Flaws

While (Temporal Key Integrity Protocol) TKIP & (a message integrity check algorithm is to verify the integrity of the packets) Michael significantly improve WEP security, design limitations result in cryptographic weaknesses.

Limitations of Michael to retrieve the keystream from short packets to use for re-injection and spoofing.

WPA2Benefits

Strong Cryptography

Support for Legacy Equipment

Strong Network Access Control

Will Support 802. 1x, EAP, EAP-TLS, Radius, and Pre-Placed Keys

Key Management

Replay Protection

Provides for data and Header Integrity

Roaming Support

Security issue

There is a flaw that was discovered. It is called WPS (wireless protected setup); it is the little initial setup that most new/newer routers come with. The WPS is a button which we need to hit when we want to initially set up connection. That is the security flaw that’s used now to crack wpa/wpa2. There is a free program to exploit this flaw (reaver) and it has about a 100% success rate in cracking wpa/wpa2.

Galois/Counter Mode (GCM)

GCM is a block cipher mode of operation providing both confidentiality and data origin authentication. It was designed by McGrew and Viega.

Benefits

Support communication speeds of 10 Gbps

Provides strong encryption based on the Advanced Encryption Standard (AES)

Be able to implement in hardware for performance and efficiency

Security Issues

GCM provides no message authentication

There are some security issues if GCM mode is used incorrectly. GCM is not suited for use with short tag lengths or a very long message. The user should monitor and limit the number of unsuccessful verification attempts for each key. It is strongly recommended to use all 16 bytes for the tag, and generally no less than 8 bytes. The same length of tag must always be used for a given key. The initialization vector (IV) must be unique for each operation for a given key. Security is destroyed for all text encrypted with the same key if the IV is used for different plaintext. Using 12 bytes randomly generated IV is ok and so is a counter that is controlled over so that it can never be repeated.

Cross layer security framework in Wireless LAN deployment

Cross-layer design appears to be a suitable approach for future contributions in the framework of WLANs – able to address emerging issues related to ever-higher performance, energy consumption, mobility.

The single layer security is often inefficient and inadequate for provisioning secure data transmission in WLAN. In generally, the security of a network is determined by the security it has over all the layers. Thus, the cross-layer security framework needs to be proposed in WLAN.

The security framework may support many components like intrusion detection system, Trust framework and adapted link layer communication protocol. In order to carry out practical cross-layer security framework in WLAN, we need to follow:

Component based security: Security measures must be provided to all the components of a protocol stack as well as to the entire network. The developers should focus on securing the entire network.

Robust, simple and flexible designs: Security mechanisms should construct a trustworthy system out of untrustworthy components and have the capability to detect and function when need arises. This should also support scalability.

Various types of active and passive attacks have been recorded in WLAN

A denial of service (DoS) attack: In DoS attack, a malicious node could prevent another node to go back to sleep mode which in turn causes battery depletion.

Eavesdropping and invasion: If no sound security measures are taken, invasion becomes fairly an easy task due to wireless communication. An adversary could easily extract useful information from the unattended nodes. Hence, a malicious user could join the network undetected by impersonating as some other legitimate node, to have access to secret data, disrupt the network operations, or trace the activity of any node in the network.

Physical node tampering leading to node compromising.

Forced battery exhaustion of a node.

Radio jamming at the physical layer.

There are some types of cross-layer securityCross-layer security design for intrusion detection

All approaches pertaining to intrusion detection schemes have been focused on routing and MAC protocols. The existing secure protocols or intrusion detection schemes are normally presented for one protocol layer. So, the effect of these schemes is sandwiched to attacks to a particular layer. They are seldom effective to attacks from different protocol layers; however, security concerns may arise in all protocol layers. It is necessary to have a cross-layer based detection framework that consolidates various schemes in various protocol layers.

Cross-layer security design for power efficiency

As previously mentioned, energy conservation is one of the primary concerns for sensor networks design, so it should be considered across protocol layers from the beginning stage through subsequent stages of the design to achieve the trade-off between energy consumption, network performance and complexity, and maximize the longevity of the entire network. Our cross-layer approach can achieve this while providing network security provisioning. For instance, the carrier detection is responsible for DoS attacks. A detrimental or malicious node can exploit then interplays in MAC layer to frequently request for channels. This not only prohibits other nodes from connecting with the destination, but also can deplete its battery energy due to frequent responses. To overcome this issue, the information can be collected from other layers and the detrimental node can be recognized and then be limited or isolated.

Conclusion

After analysing the security risks of WLAN and investigating the advantages of cross-layer security framework, I believe that the cross-layer design is a unique candidate to improve security in WLAN.

Summary

Wigig or 802. 11ad based on the 802. 11 standard is a new wireless technology which provides data rates up to 7Gbps over the unlicensed 60 GHz. It will primarily be used within a single room to provide wireless connectivity between home entertainment equipment. It will enable very fast data transfers and streaming media which is 10 times faster than the old wireless technologies. However, Wigig still has some challenges which are

the limitation of propagation loss and distance. That is why it can primarily be used within a room or an office. But Wireless Gigabit Alliance claimed that Wigig can be used beyond 10 meters by using “ beamforming” technology in the near future.