I J C T A, 9(37) 2016, pp. 651-660

Network Coding Based Smart Grids for High Level of Security in Grid Communication

Arumugaselvi Murugan*

Abstract: Encoding of the network will be a new era of communication networks, where the packets are algebraically summed rather than routed and stored in a centralized network. Based on the digital technology of the electricity distribution network called smart grid that is used to provide electricity to consumers via the digital communication bidirectional. Wireless multi-hop communications are primarily used to collect information of dosing in Smart Grids. It exchange data messages and control between the smart meters and the supplier of electricity. Any system of communication used in the smart grid should support all aspects of the protection of the private life and the intruder should not have access to the utility companies .We propose new patterns of encryption and the routing of traffic which benefit from the technology of coding of the improved network. Our analysis shows that our plans to maintain the privacy of users despite the possibility of detecting count data by an opponent. In addition, our regime has as favorable features less additional of Calculation Complexity, reliable and robust communication.

Index: Smart Grids, encryption, communication

1. INTRODUCTION

New features of the smart grid systems and networks, such as the Distributed intelligence and broad bandwidth capabilities can significantly improve the efficiency and reliability, but they can also create many new vulnerability if it is not deployed with the proper security checks. To ensure the security of such a large system may seem a task inscrutable, and if it is not done properly, can leave utilities open to cyber attacks. Based on the knowledge, solutions and standards from other systems and the industries, the best security solutions can be used for each portion of the network of communications of the smart grid. Obviously, the protocols based on the Internet, such as IPv4 and IPv6, which have been developed over the years and which have a generalized use, will provide a basis the cost-transport. Superposition of the suite of security protocols developed for IP [such as IPsec and TLS (Transport Layer Security)] on this repository transport capitalizes on the immense work done in this area by the Protocol and the experts of the industry. While the system of smart grid is composed of a number of sub-systems "energy" (Figure 1), many of the components of the communication and security, as indicated below, are common between these sub-systems

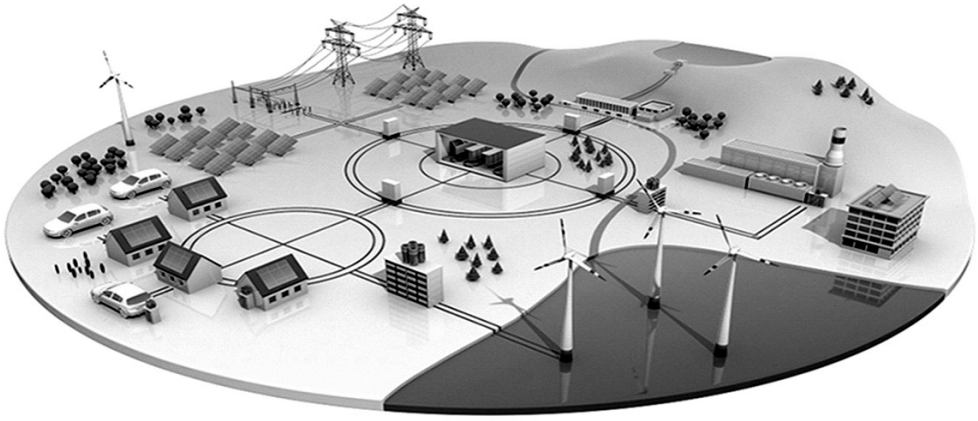

Figure 1: Conceptual Model of the smart grid

* Electrical and Electronics Engineering Department, SRM University, Kattankulathur. *Email: arumugaselvi.m@ktr.srmuniv.ac.in*

of the energy. A sub-system which is at the basis of systems for smart grid is the Supervisory Control and Data Acquisition (SCADA) solution. Several suppliers offer solutions SCADA, who have the capacity and security mechanisms. Although some standards exist around the SCADA, as distributed network.

The Intelligence of Distribution

"Distribution of intelligence" refers to the part of the smart grid which applies to the utility of the distribution system, that is to say the son, the switches and the transformers that connect the utility sub-station for you, the customers. The electrical lines which cross the people is back yards are a part of the power distribution system. A key element of the distribution The intelligence is a fault detection and response. Today, many public services rely on the telephone calls of customers to know what areas of their distribution system are affected by a power failure. With smart meters, the distribution information will help to quickly identify the source of a power outage so that teams of repair can be immediately dispatched to the area of the problem. A failure of the utility of response can also improve. Most of the utilities rely on the plans for the distribution of the power supply and complex manual switching to maintain power arising from most of their customers, even when the supply lines are damaged and destroyed. However, this approach has its limits, and in many cases, an automated system could respond more quickly and could retain the current flows up to more customers. Having sensors capable to indicate when certain parts of the distribution system have lost the power, and by combining the automatic switching with an intelligent system which determines the best way to react to a power failure, power can be rerouted to the majority of customers in a few seconds, or perhaps even in milliseconds. It may even be possible to react quickly enough to power disturbances so that only those in the immediate vicinity are affected, while other source of power of customers are redirected fast enough to avoid any interruption of the power. This capacity could be the first example of the highly-touted "self-healing" aspect of the smart grid in action.

The "Power Distribution System" of Self-healing

Response of failure is an aspect of the distribution of intelligence which is commonly called the automation of the distribution (DA). DA may actually be the oldest segment of the smart grid, because utilities have been the automation of their distribution systems since the 1960s. But while da initially focused only on the remote switches, the Electric Power Research Institute now considers the distribution to mean a fully intelligence and controllable and the distribution system flexible. Combining DA with a set of components of intelligent sensors, processors and technologies of communication will lead to the distribution of the intelligence. When it will be fully deployed, distribution intelligence will allow an electricity undertaking to monitor and coordinate its distribution assets, their optimal functioning either manual or question using the automatic commands.

Help the Grid to Operate More Effectively and Reliably

With the detection of failure and response, another potential application of the distribution is the intelligence capacity in order to optimize the balance between the real and the reactive power. Devices that store and release of energy, such as capacitors, or that the use of the coils of wire to induce the magnetic fields, such as electric motors, have the capacity to lead to an increase of the electrical currents without the use of real power; this is known as the reactive power. A certain amount of reactive power is desirable within a system of power, but too many reactive power can lead to significant flow of current that do not serve of purpose, causing losses of efficiency that they heat the wires of the distribution system. A system of intelligent distribution can use the electronic power to maintain the good level of reactive power in the system. The distribution of the intelligence can also help to protect and control the lines of input, the electricity transmission lines that make up the distribution system. Most of the supply lines are now protected by

circuit breakers or relay that trip when high currents through the line of flow, a situation normally caused by a flaw somewhere in the system.

Security Requirements

The availability of the electrical energy in North America depends in part on the availability of the power grid of the control systems. In the framework of the development of the smart grid, these control systems are more sophisticated, allowing a better control and greater reliability. Smart Grid will require a higher degree of network connectivity to support the new sophisticated features. This higher degree of connectivity also has the potential to open new vulnerabilities. In function of the Electric Power Research Institute (EPRI) [2], one of the greatest challenges facing the development of smart grid is related to cyber security systems. According to the report, "Cyber EPRI Security is a critical issue because of the potential for increased cyber-attacks and incidents against this critical sector as it becomes more and more interconnected. The cyber security must deal not only with deliberate attacks, such as of disgruntled employees, industrial espionage, and terrorists, but compromises by inadvertence of the infrastructure of the information due to errors in the user, equipment failures, and natural disasters. Of the vulnerabilities could allow an attacker to penetrate a network, access the control software.

Convolutional Encoding

To encode the data convolutional, start with *k* memory registers, each holding 1 bit of entry. Unless otherwise indicated, all the memory registers start with a value of 0. The encoder has *N* additions modulo 2 (2 modulo adder may be implemented with a single door Boolean XOR, where is the logic: 0 + 0 = 0, 0 + 1 = 1, 1 + 0 = 1, 1 + 1 = 0) and *n* – the one for polynomials of generator each adder (see figure below). A bit of entry m_1 is introduced in the registry the more to the left. Using the generator polynomials and values in the other registers, the Encoder Outputs *N* symbols. These symbols can be transmitted or pierced according to the rate of desired codes. Now the registry values of all bit shift to the right (M_1 moves to m_0, M_0 moves to m_{-1}) and wait for the next bit of entry. If there are no remaining input bits, the encoder continues of the pass until all records have returned to the zero state (Rinse the ILO termination of employment).

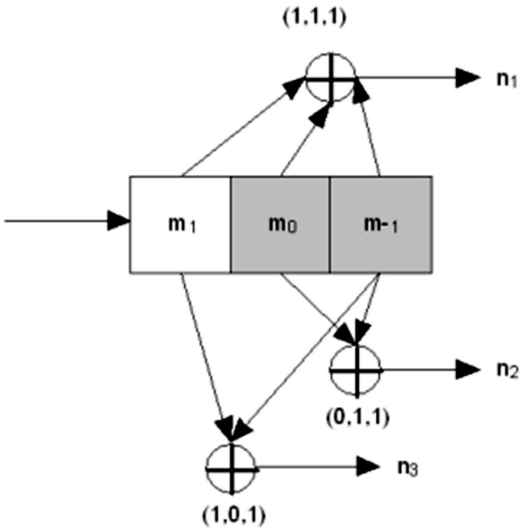

Figure 2: Convolutional Coding

Turbo Code

There are many different instances of Turbo Codes, using different encoders of component, the input/output ratios, inserts, and puncture patterns. This example describes an implementation of the Encoder classic turbo

and demonstrates the encoder general design of Turbo Codes parallel. This encoder application sends three sub-blocks of bits. The first sub-block is the block bit M- of payload data. The second sub-block is $n/2$ bits Parity for the payload data, calculated using a convolutional code recursive systematic (Code RSC). The third sub-block is $n/2$ bits Parity for a permutation of the known payload data, once again calculated with the aid of a code of the RSC. As well, two redundant, but different sub-blocks of parity bits are sent with the payload file. The complete block has $m + n$ bits of data with a code rate of $M/(M + N)$. The permutation of the payload data is carried out by a device called a interleaver . Hardware-wise, this turbo-code encoder consists of two coders CSR identical, C_1 and C_2, as shown in the figure, which are connected to each other with the aid of a diagram of concatenation, called *Parallel concatenation*:

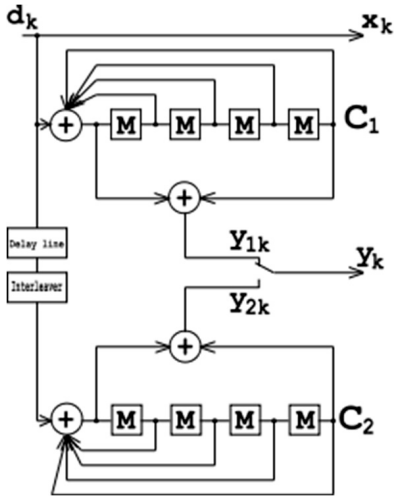

Figure 3: Code of Turbo

Coding of the Network

The coding [4] network is often used to illustrate how the coding linear network can be more efficient than the routing. Two nodes source (at the top of the image) have information A and B which must be transmitted to the two destination nodes to (bottom), each of which wants to know A and B. Each edge can carry only a single value (one can think of an edge transmitting a bit in each time interval). If only the routing were allowed, then the central link would only be able to carry a or b, but not both. Suppose that we send a Through the Center; and then the left could receive a destination twice and do not know B to all. The sending B poses a problem similar to the correct destination. We say that the routing is insufficient because no routing scheme can transmit both A and B simultaneously to two destinations. Using a simple code, as shown, A and B can be transmitted to the two destinations simultaneously by sending the sum of

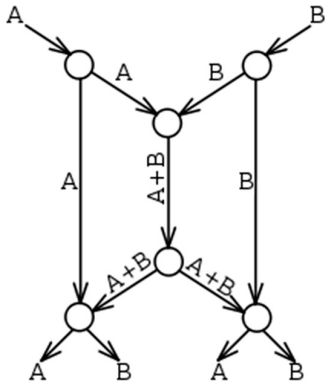

Figure 4: Encoding of the network

symbols through the center - in other words, we encode A and B using the formula "A+B". The destination of the left receives a AND A + B, and can calculate B by subtracting the two values. Similarly, the good destination will receive B and A + B, and will also be able to determine the two A and B. A similar concept has been used to encode stereophonic sound, where there is a signal "left" and "right" of the signal. The two analog signals are "added" together, and the "sum" is subsequently used to retrieve the signals of origin.

A. The Security Based on Coding of the Network

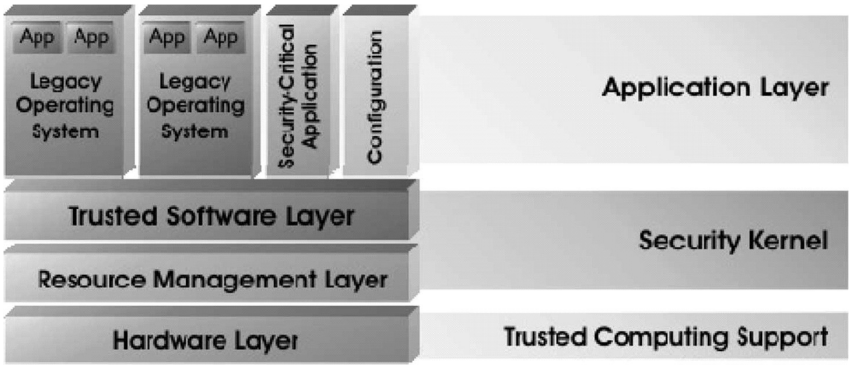

Figure 5: Trusted Computing Model

The PKI is a powerful tool that can be used to secure the in-Tication and the authorization for a security association (SA) and the establishment of keys. The ICP can, however, be notoriously difficult to deploy and operate. This is mainly because the standards of the ICP (such as X.509 and IETF RFC 5280) only provide a high level framework for the use of digital certificate and for the implementation of a PKI. For example, they do not specify how a particular organization should approve the certificate signing requests, or how the organization should protect each CA. They provide a mechanism for defining the naming conventions, certificate constraints, and certificate policies, but they do not specify how they should be used. These standards legitimately leave these details to the organizations responsible for implementing the PKI, and work on all of these details is where a large part of the expenditure is incurred. Some industries (such as the financial services industry) have standardized a political model of PKI. The objective of a political model is to define the naming conventions, constraints, policies, and many operational aspects of a PKI infrastructure for an entire industry. Not only will this have important benefits for the interoperability, but just as significantly, it will ease the burden of the implementation, because each organization will not have to independently of the search of the PKI and to identify policies and practices for themselves. They will have been determined by the industry, and they will be known to have the desired level of security. We therefore propose the development of standards of PKI for use by the industry of critical infrastructure. The standards would be used to establish requirements on PKI operations of suppliers of energy services (e.g., utilities, generators, ISO) as well as the manufacturers of appliances for smart grid. The standards could include elements such as the strategies of security acceptable (e.g., policies of certification of the ICP used for the issuance of each type of certificate in the system), the formats of certificate, and the practices of the PKI.

B. Security Trust Anchor

One of the main components of a compatible system secure PKI is the requirement that each RP (Any device that uses the certificate of a second part to authenticate the second part) must have secure methods to load and store the root of trust or anchor of confidence (TA). The TA is generally a CA to the top of a hierarchy of Certification Authorities. RPs holders of certificates of trust because they have confidence in the TA, which trusts a CA, which trusts the end certificate holders. This confidence is attested by a chain

of root certificates on the anchoring of trust. If an opponent could modify the root of trust for any RP, that RP could easily be compromised. We propose that each operator will support its own PKI hierarchy with its TA at the top. The challenge for the operator is to ensure that each secure device obtains the information on ta correct. A method to do this without having to manually the preload of the TA Certificate in each device is as follows. Each factory production should accredited the preload of the device using a certificate, to identify the manufactures the brand, model and Serial number of the device, as well as a preprovisioned TA certificate. After a smart grid operator buys a smart grid terminal, Manufacturer Makes the operator a TA certificate, transfer which would instruct the device to accept the root CA certificate of the operator as the new trust anchor, and only the operator's root CA certificate. The TA certificate of transfer would be limited to specific devices (from serial number). The tools automate the entire process of transfer, to reduce ta the EF-fort to potentially be as simple as putting the unit under tension in the network of the operator, of the send the address of the TA repository of transfer of [possibly by the intermediary of a domain name server (DNS)], and al-bellowing it to automatically request the certificate of transfer and new TA certificate. For devices to be very critical it is recommended that the device must have a HSM fips to safely store the TA certificate. The model is used to format your paper and the style of the text. All the margins, the width of the columns, Spacing, and text fonts are prescribed; please do not modify. You can note peculiarities. For example, the margin of head in this model measures proportionately more than 'habit. This measure and other are deliberately, using the specifications that anticipate your paper as a part of the whole of the procedure, and not as a document independent. Please do not revise the current designations.

3. THE PROPOSED SOLUTION -TRUSTED COMPUTING

The North American electrical grid is currently the subject of a major transformation. By adding new functions, of a distributed intelligence, and state-of-the-art software capabilities of communication to broadband, the grid can be rendered more effective, more resilient and more affordable to manage and operate. Unfortunately these same capabilities will greatly increase the number and the type of threats to which the grid will be exposed. Given the large size of the scope and the breath of the smart grid, it is reasonable to expect that the cumulative effects of the vulnerability of the system can also be very broad. Virtually all of the Parties agree that the consequences of a Smart Grid cyber security. New functions such as the answer to the request to introduce significant new vectors of attack such that a malicious software that launches a huge coordinated and decline in the instant application, poten-potentially causing substantial damage to the distribution, transmission, and even the facilities of generation.

In the light of the incredible importance of the threat and vast potential consequences of cyberattacks, the smart grid cybersecurity protection requirements must be extreme. The grid will require a comprehensive security plan that encompasses virtually all the aspects of the operation of the grid. An element of this plan includes trusted computing platforms. Figure 3 shows a computer model of confidence of base [1]. Such platforms and associated mechanisms are used to ensure that malware is not introduced in a treatment software for the devices.

There are two categories of devices for which the malware protection problems should be studied: embedded computing systems and computer systems in general use. Embedded systems are computer systems that are designed to perform a specific task or a set of tasks. They are designed to operate only a software which is provided by the manufacturer. By contrast, the purpose general systems are intended to support third-party software pure chased by consumers who have purchased the system. A PC is an excellent example of a system for general use. A microwave oven, television by cable or set-top box, are examples of integrated systems. The problem of the protection against malicious software should be considered separately for each category.

For embedded systems the problem of protecting the system against the installation of malicious software can be resolved with a high creek of insurance. First and foremost the manufacturer must implement software development process secure; many standard models for these processes are defined in [8]. Secondly, if the device is the intention to be upgraded on site, the manufacturer must provide a solution to upgrade the secure software. The main method to do this is to manufacture equipment integrated systems with a secure storage containing the hardware encryption for a validation of the software. In general, the hardware is configured with the public key of a Secure Signing Server operated by the manu-invoicing. With this key, the device can validate any newly downloaded the software before the run. Such a proactive approach can provide higher levels of assurance that can be obtained with a reactive approach such as a antivirus.

Additional security can be obtained by validating the software each time that the device starts up. These techniques are referred to as high assurance boot (HAB). HAB techniques typically rely on core software in the secure hardware to validate code of boot block. The Code of start lock then validates the operating system (OS), and the OS to its valid tower higher-level applications. Each step of validation is performed using the public key or keys preinstalled in the secure hardware.

For devices which are designed to operate for long periods of time (e.g., years) without starting, it is useful to have a method to perform a secure software validation on the execution of code. It is possible to have background tasks that can run periodically these functions without disrupting the operations of the device. In addition, it is possible to couple such as the steps of validation of substance with other operational aspects of the device, such that if the Of- vice is found to be compromised, the secure hardware on the device (necessary to put in place and maintain security associations with Re-mote entities) will prevent the local device of the establishment and maintenance of security associations with the remote entities. Many documents, such as [9], are available on the ways to provide the attestation of remote device.

Attestation of device is necessary to ensure, for the devices on the network, their true identity, before any manual or auto-provisioning connected to the site.

With the device, accredited manufacturers technical certification can factory install Certificates of attestation of device in each device of the smart grid. These device security certificate is only used for the certification of affirm the device manufacturer, model, serial number, and that the device has not been tampered with. These certificates neck with the pled-authentication protocol can be used by the supplier of energy services in order to ensure that the device is exactly what it claims to be. In order to support device certification, the device will need a hardware security module FIPS 140 (HSM), and will need the functionality of the HAB.

For computer peripherals for general use, such mechanisms allowing only the software approved by the manufacture of run have not been popular. The consumers of PCs in general believe that they should not be limited by the manufacture of load software they want, even if it means having to put in place with malicious software attacks. The principal means of protecting net-worked PCs has been to use the detection of malicious programs and removing soft-ware typically designated as antivirus software. One of the most effective tools that uses the antivirus software to detect malicious software is a “signature” dictionary. The term “signature” is used here to designate a model code recognizable, as known op-posed to the cryptographic signature used above. With the signature dictionary, only known viruses can be discovered and re-moved. Such methods are not useful in the protection against new, unknown viruses. Obviously with the Poles if high, the smart grid needs a better solution than the reagent dictionary approach antivirus.

To make things worse, the rapid adoption of cloud computing and applications based on sophisticated Internet has resulted in the widespread deployment of a number of “mobile code” technologies. Mobile Code is a code that is downloaded and executed on your computer, usually by your browser, without the authorization of the user knowledge. Examples of mobile code include Active X, Flash, ANIMA-tion,

Java, JavaScript, PDF, Postscript, and Shockwave. The Department of Homeland Security (DHS) program of the security of the system of control [10] recommends strict controls on the mobile code in the control systems-ical Crit for the essential infrastructure of our country and the main resources (CIKR).

To respond to this concern, we propose the adoption of', and adherence standards of signature of strict code by the operators and suppliers of smart grid. Mechanisms to apply these standards on computers to general use, such as PC, have been put forward by the Trusted Computing Group and are well documented [11]. These standards should cover all the devices in critical state, including units deployed on the ground, such as the licensing of use and of FDI, network devices, such as routers, switches, and firewalls, and the control center of the equipment, such as servers and user consoles. The standards should focus on the embedded systems, as well as general purpose computers, their operating systems, drivers, and applications, as well as all the Mo-bile code. It is, not of mobile code should be allowed to run on a PC or a critical server that has not been signed by an authority that is able to determine the reliability of the Code. Considering that it is certain that the hardware and software for the critical components of the GRID will come from many different suppliers, it is likely that a framework for the management of the confidence will need to be established for the smart grid. This framework will probably require the establishment of a set of criteria which are to be respected by the suppliers who wish to sell of the elements critical to the operators of the smart grid. In addition, it is likely that one or several organizations of station of accredi will need to be established for audit suppliers to determine that they meet the criteria specified.

4. CONCLUSION

As a critical infrastructure element, smart grid requires the highest levels of security. A comprehensive architecture with security built in from the beginning is necessary. The smart grid security solution requires a holistic approach including PKI technology elements based on industry standards, and trusted computing elements. PKI technical elements, such as certificate lifecycle management tools, trust anchor security, and attribute certificates, are known technologies that can be tailored specifically to smart grid networks, resulting in an efficient and effective solution. The PKI solution supports the trusted computing elements, including device attestation.

To achieve the vision put forth in this paper, there are many steps which need to be taken. Primary among them is the need for a cohesive set of requirements and standards for smart grid security.

References

1. R. Rejaie and S. Stafford, "*A Framework for the design of the peer-to-peer architecture receiver-driven*", Nossdav SUPERIMPOSITIONS 04, Ireland, June 2004.
2. K. Jain, L. Lovasz, and P. A. Chou, "*Building robust and scalable a peer-to-peer for broadcasting overlay networks using Network Coding*", symposium of the AGR on the principles of distributed computing, Las Vegas, 2005.
3. P. A. Chou, Y. Wu and K. Jain, "*Network coding for the Internet*", Workshop on the theory of IEEE Communication, Italy, May 2003.
4. Http://www.akamai.com
5. Ying Baochun Zhu, Li, Jiang Guo, "*Multicast with Network coding in networks of superposition of Application layer*", Journal of the IEEE on selected areas in communications, January 2004.
6. P. A. Chou, Y. Wu and K. Jain, "*practices*", network coding Allerton conference on communication, control and computing, Monticello, HE, October 2003.
7. Zongpeng Baochun Li, Li, Dan Jiang and Lap Chi Lau, "*On the achievement of optimal end-to-end the flow in the data networks: theoretical pirical and EM-studies*", technical report of the EEC, of the University of Toronto, February 2004.
8. R. Ahlswede, N. Cai, S. R. Li, and R. W. Yeung, "*network information flow*", IEEE Transactions on the theory of information, July 2000.

9. Mr. Castro, P. Druschel, A.-M. Kermarrec, A. Nandi, A. Rowstron and A. Singh, "*SplitStream: High-Bandwidth multicast in the co-operative environments*", Proc. of the 19th ACM Symposium on the principles of operating systems (SOSP), October 2003.
10. V. Padmanabhan, H. Wang, P. cabbage, and K. Sripanidkulchai, "*Distributors-ing of multimedia content continuously to the help of co-operative networks*", Proc. of NOSSDAV 2002, May 2002.
11. J. Byers and J. Considine, "*Informed content delivery in the whole of the networks of overlay adaptive*" Proc. of SIGCOMM ACM, August 2002.
12. D. Kostic, A. Rodriguez, J. Albrecht, and A. Vahdat, "*bullet: the dissemination of high-bandwidth data using a bottom of page mesh*", Proc. of the 19th ACM Symposium on the principles of operating systems (SOSP 2003), 2003.
13. Paul Francis, "*Yoid: extension of the Internet multicast architecture*", Document not published, April 2000.
14. Yang-hua Chu, Sanjay G. Rao, and Hui Zhang, "*a case of end multicast system*", Proceedings of the ACM Sigmetrics, Santa Clara, CA, June 2000, pp. 1-12.
15. Vivek K Goyal, "*Multiple Description: Compression of coding meets the network*", IEEE Signal Processing Magazine, May 2001.
16. B. Cohen, "*Incentives build robustness in BitTorrent*", P2P Economics, 2003. The workshop
17. Rob Sherwood, Ryan Braud, Bobby Bhattacharjee, "*Slurpie: a coop-erative data transfer protocol in bulk*," IEEE INFOCOM, March 2004
18. P. Rodriguez, E. Parallel-Access Biersack, "*Dynamic for replicated content in the Internet*", IEEE Transactions on Networking, August 2002
19. John Byers, Michael Luby, and Michael Mitzenmacher, "*Access to several sites mirrors in parallel: Using Codes Tornado to accelerate downloads*", INFOCOM 1999.
20. Mr. Izal Urvoy-Keller, G., E.W. Biersack, P. Felber, A. Al Hamra, and L. Garces-Erice, "*dissect BitTorrent: five months in a Torrent's lifetime*", passive and active measures 2004, April 2004.
21. Mr. N. KROHN, Mr. J. Freedman, and D. Mazieres", "*on-the-fly rateless checked-cation of clearing codes for the distribution of the content effective*" IEEE Symposium on Security and the protection of the private life, 2004
22. Dongyu Qiu, R. SRIKANT, "*Modeling and performance analysis of bitTorrent-Like peer-to-Peer Networks*", in Sigcomm 2004.
23. John W. Byers, Michael Luby, Michael Mitzenmacher, and Ashutosh Rege, "*an approach Digital Fountain The reliable distribution of data in bulk*", SIGCOMM, 1998.
24. Petar Maymounkov Mazires and David, "*Rateless Codes and IPTPS Big downloads*", "03, February 2003.
25. K. Jain, Mr. Mahdian, and Mr. R. Salavatipour, "*Packaging Steiner Trees*", Proceedings of the 10th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 2003.
26. G. Robins and A. Zelikovsky, "*the improvement of the tree Steiner approximation in graphics*", Proceedings of the 7th Annual ACM-SIAM Symposium on Discrete Algorithms (SODA), 2000.
27. Mr. Thimm, "*on the Approximability of the problem of the tree Steiner*", Mathematical Foundations of informatics 2001, Springer LNCS, 2001.
28. T. Ho, R. Koetter, Mr. Medard, D. Karger, and Mr. Effros, "*The advantages of the coding on the routing in a random parameter*", ISIT, Yokohama, Japan, 2003.
29. G. Pandurangan, P. Raghavan and E. Upfal, "*Construction of small diameter P2P networks*", 42nd Annual Symposium on the foundations of the informatics (FOCS01), pp. 492-499, 2001.
30. Mr. Krohn, Mr. Freedman, D. Mazieres, "*on-the-fly the Rate Check-codes of clearing for efficiency less Content Distribution*", IEEE Symposium on Security and the protection of the private life, Berkeley, CA, 2004.
31. E. Adar, B. Huberman, "*free riding*", first Gnutella on Monday, available at: http://www.firstmonday.dk/issues/issue5 10/ Adar/, 2000.
32. Mr. Bellare, J. A. Garay, and T. Rabin, "*Audit of the fast batch modular and digital signatures the exponentiation*", the progress in the areas of cryptology, 1998.
33. P. Felber, and E.W. Biersack. "*Auto-scalability of content distribution networks*", in Proceedings of the International Workshop on self-* in complex information systems of the properties (auto-*), Italy, 2004

34. C. Gkantsidis, and P. Rodriguez. "*Large-scale of coding of the Content Distribution network*", in IEEE/INFOCOM 2005.
35. S. Deb, C. Choute, Mr. Medard, and R. Koetter. "*How is good coding random linear founded the distributed networked storage*?, NetCod 2005
36. T. P. Pedersen "*non-interactive and the theoretical information checked secure-capable shared secret*", progress in the areas of cryptology Crypto, 1991.
37. D. Chaum, E. van Heijst, and B. Pfitzmann, cryptographically strong undeniable signatures, for the'sécurisé without condition signatory, advances in cryptology Crypto, 1991.
38. J. Benaloh, and Mr mare, "*one-way Accumulators: an alternative to digital sinatures decentralized*", progress in the areas of cryptology Eurocrypt 93, 1993.
39. N. Baric and B. Pfitzmann, "*without collision accumulators and wiring diagrams of signature failstop without trees*", advances in cryptology Eurocrypt 97, 1997.
40. Mr. Micciancio Bellare and D., "*a new paradigm for the hash collision-free: the incrementality at a lower cost*", the progress made in the areas of cryptology ROCRYPT EU-97, 1997.
41. S. Micali, and R. Rivest, "*transitive*", diagrams for the signature of the progress in the areas of cryptology RSA CT 2002, 2002.
42. R. Johnson, D. Molnar, D. song, and D. Wagner, "*patterns of the homomorphic signature*", the progress in the areas of cryptology RSA CT 2002, 2002.
43. R. Canetti, J. Garay, G. Micciancio Itkis, D., Mr. Naor, and B. Pinkas, "*Multicasting: security a taxonomy and some constructions effective*", Proc. IEEE INFOCOM 99, 1999.
44. C. Karlof, N. Sastry, Y. Li, A., and J. Tygar Perrig, "*Codes of distillation and applications to multicast authentication resistant DoS*," in Proc. 11e Networks and Distributed Systems Security Symposium (NDSS), San Diego, CA, 10 Feb 2004.
45. R. Merkle, "*Protocols of cryptosystems to public key*", Proc. of the IEEE Symposium on research in the field of security and confidentiality, AVR. 1980.
46. Christos Gkantsidis, Milena Mihail, Amin Saberi, "*the conductance and congestion in the graphs in a power-law*" ACM SIGMETRICS, 2003.
47. P. Mazieres Maymounkov and D., "*Kademlia: A peer-to-peer of the informa-tion based on the metric system XOR*", in Proceedings of IPTPS02, 2002.
48. A. Rowstron and P. Druschel, "*pastry: Scalability and distributed the location of the object and the routing for wide-scale peer-to-peer systems*", the IFIP/ACM International Conference on the platforms of distributed systems (middleware), 2001.