Detection of PARD Attack on Secure Authentication System Based on Fingerprint Impression

Indu Verma* and A.K. Vatsa**

*AKGEC, Ghaziabad, (U.P) INDIA.
**Department of Computer Science, University of Missouri, Columbia, MO, USA
Email: induverma029@gmail.com, avimanyou@rediffmail.com

Keywords: Biometrics, Fingerprint, Security, Authentication, PARD attack, Minutiae features, Encoding, Decoding.

Abstract: The trustworthy information security mechanisms are required to contend with the rising atrociousness of identity theft in the cyber and electronic society, the biometric like fingerprint authentication can be used to ensure that only the legitimate user can access to intended system. Although the biometric authentication systems are very secured but the biometric systems are also exposed to a number of attacks like ersatz feature attacks, Brute force, Hill climbing attacks, Replay attacks, Latent print attacks, worm attacks, Dead feature attacks, Software leaks and Use of force attacks are most typical and vital to biometric security parts, so it is important to address the issue of secure design of the biometric system. Therefore, in this paper a PARD attack on secure authenticated system to identify that the system is able to detect the attack done by the interlopers is proposed. Thus, a combination of extracted fingerprint features and biocrypto key will entail generating a secure authentication system based on fingerprint impression meant for PARD attack using fingerprint verification through extracting and matching minutiae, and to incorporate the instability of the user’s biometric features into the generated key, so as to make the key unguessable to an attacker lacking significant knowledge of the user’s biometrics.

1. Introduction

Biometrics has gained a lot of importance; the reason is that it is the only means of identification of a biological entity by a non-biological entity e.g. a computer machine. With the advent of extensive use of computer machines for secure transactions through cyber crimes the various important data like e-mails, e-banking, e-purchasing, etc. and correct identification of the user is very important. The prevalent systems use mostly passwords directly as a key for the cryptosystem or sometimes they use the password to get an access to the password stored in some smartcard possessed by the user. The major loophole in using such a security is that these passwords being very simple can be remembered by any user and hence are prone to be compromised as most of the time these passwords are easy to guess. Also carrying a number of smartcards which contain the key is very inconvenient. Using password or key itself is very vulnerable, take credit cards for instance, any good hacker can install key-loggers or other such software on one’s system and can have access to credit card number and any other information that one might not want to share.

Another big problem with the prevalent cryptosystems is repudiation of the illegal things done by people over the electronic media. Either people don’t identify themselves correctly while creating an account with some server which they are eventually going to disavow after doing some illegal things, or they simply escape by saying that somebody stole their password. Biometrics completely depicts the identity of the person and eliminates the case of non-repudiation; also there is no need to remember long passwords. But these benefits can be redeemed by their proper usage only.

In forensics, criminal identification and prison security are some of the applications which employ biometrics in a comprehensive manner. In fact, a broad range of civilian application areas are utilizing biometrics. Biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of a specific physiological or behavioral characteristic possessed by that person.

The generic criteria for gathering the fingerprint credentials can be divided into five subsystems: Data collection, Transmission, Data storage, Signal processing and decision systems.

Data Collection: This subsystem uses a sensor or camera to acquire the image of the fingerprint of the user.
Transmission: This subsystem transmits the data collected from data collection module after compressing it, to the data storage and signal processing module.

Data Storage: Stores the image and template of the user.

Signal Processing: This is the most important module of the system. It performs feature extraction by image processing techniques and pattern matching operations.

Decision: This module performs identification or verification by using the match scores.

There is a requirement to emphasis on the important issues of data processing and authentication to merge biometric and cryptography for binding and generating bio crypt. The performance of bio crypt based systems is dependent on the quality of the enrolled biometric. Enrolment quality can be affected by accidental or deliberate events and environmental conditions, and the result of low enrolment quality is almost inevitably due to poor system performance. If the performance is poor the security will be compromised, and there may be excessive dependence on the fallback system.

Diverse biometric techniques that are under research include fingerprints[14], facial[15], palm prints, retinal and iris scans[16], and hand geometry[17], signature capture and vocal features[18]. With the help of this information’s the fake person and authorized person can be easily identified. This information is related to human body and their structure which are unique in this earth[18,34]. The fingerprints are eternally associated with a user and cannot be replaced, through various studies it has been observed that no two persons have the same fingerprints, hence they are unique for every individual. Ultimately, a cryptographic key in combination of fingerprint impression generation is required to make the system secure, therefore the system based on the fuzzy vault is constructed. The cryptographic key thus generated will be irrevocable and also will provide increased protection in cryptography based security systems[3]

This paper is organized in Chapters. The introduction of Bio-metric information, security and authentication etc are discussed under the heads of the Introduction in Chapter 1. The Backgrounds of this paper is mention in Chapter -2 that includes the literature review of this paper. The chapter 3 mention the proposed architecture and mechanism for Detection of PARD attack on secure authentication system based on fingerprint impression under heads of Proposed Work. The Chapter-4 concluded this paper and mention further enhancement of this paper under heads of future scope in chapter – 5. Finally, all the references used in this paper are included in Chapter -6 under heads of references.

2. Background

This work is motivated by variety of earlier researchers with their work existing within the literature regarding fingerprint biometrics, cryptography and cryptographic key generation.

The efficient and effective mechanism for confidentiality and authentication for biometric information[1] enhances the speed of encryption, decryption and authentication process. It uses arithmetic encoding scheme and public key cryptography e.g. modified version of RSA algorithm called RSA-2 algorithm[34], the bio-metric information is converted into integer real values and encodes this value with arithmetic coding[38]. Which produces integral length code and result is in floating point number. This can provide more security because the probability of alphabet or decimal number is set by the user and it is known only to authenticated person.

The fingerprint recognition can be understood by an effort to how Fingerprint Recognition[29] is used as a form of biometric to recognize identities of human beings. It includes all the stages from minutiae extraction from fingerprints to minutiae matching which generates a match score.

The authors have presented a partial thinning scheme to reduce the computation of thinning, and implement a fingerprint recognition system based on this partial thinning scheme[80]. The real time fingerprint recognition system consists of four stages: pre-processing, image enhancement, minutiae extraction, and minutiae matching.

Biometric technique as an automated methodology[19] for the recognition of a person based on behavioural or physiological characteristics is presented. The authors concluded that biometric technologies are now the key to an extensive array of highly secured identification and personal verification solutions[2].

The basics of fingerprint biometric modality[32], its applications, and the various methods for extracting minutiae points from input fingerprint images are presented in detail. Further the paper represents ways for generating the strong bio-crypt key based mostly on fingerprint. Fingerprint biometric modality is predominantly thought of due to its two vital characteristics uniqueness[39] and permanence that’s ability to stay unchanged over the lifetime.

Comparison among the traditional security systems[11] with biometric systems is discussed. The lack of secrecy (e.g., leaving fingerprint impressions on the surfaces we touch), and non-replace ability (e.g., once the biometric data is compromised, there is no way to return to a secure situation, unlike replacing a key or password) are identified as the main problems of biometric systems.
3. Proposed Work

A. Architecture and working of Detection of PARD attack on secure authentication system based on fingerprint impression:

A biometric system is embedded in the authentication process of an identity management system. Its result is used to decide if the individual that has delivered the biometric process of an identity management system. Its result is used to decide if the individual that has delivered the biometric data shall be recognized by the identity management system. The flow of the data in the Fig. 2 is as follows:

1. Take fingerprint impression as input.
2. Extraction of Minutiae points from fingerprint is done in four parts:
   a) HistofMedian method is used to enhance the fingerprint image
   b) Binarization is applied on the enhanced image.
   c) Region of Interest is extracted by using morphological operations.
   d) Using Thinning algorithm features are extracted from digitized data.
3. On the extracted features now apply key KFV to encode the feature vector.
4. At the same time an attack named PARD attack hit the secured system but as the features are encoded with the key so it will be detected by the matcher.
5. A Matcher is a comparison process that evaluates the similarity between the reference templates residing in the database and the captured data sample and that result in a similarity score.
6. Assume that the data available in Fingerprint database is also encrypted with the same i.e by key KFV at the time of enrollment of the person.
7. If the authentication process authenticates the person who want to use the application device, the secret features will be extracted now and will be available to the application devices, otherwise the authentication process will not allow the person to use the data.
8. The key will not get released just after extraction of the features because of the security issues, in fact key will be released on the same side of the application device, otherwise meanwhile an attack can hit on the secret data.

B. Working Principle:

It is divided into four parts – preprocessing of Fingerprint Image, key generation, authentication and PARD attack.

1) Preprocessing of Fingerprint Image:

a) Fingerprint Image enhancement: This technique is used to make the image clearer for easy further operations. Since the fingerprint images acquired from sensors or other Medias are not assured with perfect quality, those enhancement methods, for increasing the contrast between ridges and furrows and for connecting the false broken points of ridges due to insufficient amount of ink, are very useful for keep a higher accuracy to fingerprint recognition. HistofMedian image enhancement Method is adopted for image enhancement stage i.e for contrast expansion, in this method histogram image array is created, divided the image into two sub images based on median, calculate cumulative image histogram and performed Fast Fourier Transform (FFT) according the formula given below.

\[ F(u,v) = \sum_{x=0}^{M-1} \sum_{y=0}^{N-1} f(x,y) \times \exp \left\{ -j2\pi \left( \frac{ux}{M} + \frac{vy}{N} \right) \right\} \] (1)

In order to enhance a specific block by its dominant frequencies, the FFT of the block was multiplied by its magnitude a set of times.

Where the magnitude of the original

\[ FFT = \text{abs}(F(u,v)) = |F(u,v)| \]

The enhanced block is obtained according to

\[ g(x,y) = F^{-1} \{ F(u,v) \times |F(u,v)| \} \] (2)

The \( k \) in formula (2) is an experimentally determined constant, which was chosen as \( k = 0.45 \) to calculate. While having a higher “\( k \)” improves the appearance of the ridges, filling up small holes in ridges, having too high a “\( k \)” can result in false joining of ridges. Thus a termination might become a bifurcation. The transformation of the two sub images is to be computed now and after obtaining the enhanced block rescan the image and write the output.

b) Binarization of Enhanced Image: Translation of a grey level image into a binary image is done by a
process called binarization [6], i.e., Fingerprint Image Binarization is to transform the 8-bit Gray fingerprint image to a 1-bit image with 0-value for ridges and 1-value for furrows. After the operation, ridges in the fingerprint are highlighted with black colour while furrows are white. A locally adaptive binarization method is performed to binarize the fingerprint image. Such a named method comes from the mechanism of transforming a pixel value to 1 if the value is larger than the mean intensity value of the current block (16x16) to which the pixel belongs.

c) **ROI extraction by Morphological operations:** For ROI extraction from the binary fingerprint image, the morphological opening and closing operations are to be applied using a structuring element. The morphological operators\(^1\) will throw away the leftmost, rightmost, uppermost and bottommost blocks out of the bound, so as to get the tightly bounded region just containing the bound and inner area. The bound is the subtraction of the closed area from the opened area.

Two Morphological operations called ‘OPEN’ and ‘CLOSE’ are adopted. The ‘OPEN’ operation can expand images and remove peaks introduced by background noise. The ‘CLOSE’ operation can shrink images and eliminate small cavities.

d) **Feature extraction from digitized data:** The minutiae points are extracted from the preprocessed fingerprint image using Thinning. Thinning is defined as a morphological operation in which the foreground pixels are eroded in succession till they are one pixel wide. The Ridge Thinning algorithm is made use of in the proposed approach for Minutiae points’ extraction. It extracts minutiae points by getting rid of the redundant pixels of ridges until the ridges become just one pixel wide.

2) **Key Generation Mechanism:** The biometric system is also vulnerable to a number of adversary attacks, it is important to address the issue of secure design of the biometric system. Biometrics based key generation method, is that since secret and biometric templates are securely stored in the crypto biometric template, the system is less vulnerable to attacks on the template information database. When biometric identifiers are employed as “keys” in the context of the cryptographic system, demanding such exactitude is impractical, that is, for the same biometric entity that is analyzed during different acquisitions, the extracted biometric data will significantly vary due to acquisition characteristics. The key generation mechanism is shown in Fig 1.

3) **Authentication Mechanism:** Security of access control involves authentication of user and of the application. A user through some sensing devices like fingerprint scanners, smart card readers etc., gathers credentials\(^1\). Then the access control system offers authentication as security service and also many more.

In the authentication mode, the system authenticates an individual by searching the templates of the users stored in the database for a match. Therefore, the system conducts a one-to-many comparison to authenticate an individual’s identity without the subject having to claim an identity.

4) **Detection and Attack:** In spite their abundant advantages, biometric systems are vulnerable to attacks, which can decrease their security\(^1\). The discussed attack system inputs synthetic minutiae sets to the matcher with the aim of gaining access to the system in place of a genuine user. Note that the user’s template information is unknown to the attack system. Using the scores returned by the matcher and the characteristics of these minutiae sets, the attack system tries to generate a minutia set that results in a sufficiently high matching score to achieve positive identification. In this paper the PARD attack is discussed, the term PARD is an abbreviation to four operations(Perturbing, Adding, Replacing, and Deletion) which can be performed on the secure data to prevent access of the authorised users, the block diagram of the attack system is given in Fig 3.
C. Mechanism for Detection of attacks on secure authentication system:

The proposed mechanism is described in following four phases:

Phase - 1: Fingerprint Impression as input for Authentication:

**Step-I:** Take samples of fingerprint Impression for authentication of intended user.

- **Step-II:** Fingerprint Image Enhancement
  - Create and initialize histogram array.
  - Calculate the histogram median ($H_{MD}$).
  - Divide the image array $H$ of a section with gray level of $H = H_T$, and two sub images will be $H_L$ and $H_U$ based on the median $H_{MD}$.
  - $H = H_L U H_U$, Here $H_L = (H(i,j) | H(i,j) < H_T, \forall H(i,j) \in H)$ (H (i,j) | H (i,j) ≥ HT, \forall H (i,j) ∈ H)
  - Scan every pixel and increment count.
  - $Count++$
  - Form the cumulative image histogram.

- **Step – III:** Binarization of enhanced Image
  - An initial threshold ($Th$) is chosen randomly.
  - $Bin\_image(Th)$
    
    ```
    if (f(m,n)>Th)// f(m,n) is the pixel value located in the n,mth column, nth row
    G1 = f(m,n) // object pixel
    else if (f(m,n)<=Th)
    G2 = f(m,n) // background pixel
    m1 = avg( G1) // The average of each set is computed.
    m2 = avg(G2)
    Th’ = (m1 + m2)/2
    if(Th(aprx)!=Th)
    {
    Bin\_image(Th’)
    //keep repeating until the new  threshold Th’ matches the one before it Th.
    }
    }
    ```

- **Step –IV:** Segmentation of digitized values
  - ROI extraction by Morphological operations: To extract the ROI, a two-step method is used. The first step is block direction estimation and direction variety check, while the second is intrigued from some Morphological methods.
  - Scanning the skeleton of fingerprint image left to right and top to bottom
  - $Bound = openArea - closedArea$
  - $L2R = sum(Bound)$
  - $roiCol = find(L2R>0)$
  - $left = min(roiCol), right = max(roiCol)$
  - $tr\_bound = bound’$
  - $top2dw = sum(tr\_bound)$
  - $roiRow = find(top2dw>0)$
  - $top = min(roiRow), bottom = max(roiRow)$
  - Cut out the ROI region image and show background, bound, innerArea with different grey intensity by setting it equal to 0,100,200
  - for $i =$ top to bottom
  - for $j =$ left to right
  - if (Bound(i,j) == 1)
    
    ```
    template(top,bottom,left,right) = 200;
    tmp(top,bottom,left,right) = 1;
    ```
  - else
    
    ```
    if (Bound(i,j) == 1)
    template(top,bottom,left,right) = 100;
    tmp(top,bottom,left,right) = 1;
    ```

- **Step – V:** Feature extraction from digitized data
  - Scanning the skeleton of fingerprint image row by row...
Phase – II: Encoding and Decoding with Key Generation Mechanism: It can be summarized a biometric (fingerprint) key generation system, a cryptographic construct called the fuzzy vault[3]. For simplicity, assume that the system uses 8-bit –coordinates of fingerprint minutiae features but it can be (and has been) extended to include other minutiae information as well. Further assume that x-coordinates have been appropriately coarsely quantized (e.g., to the nearest number divisible by 5).

Encoding: Fig 4 shows the Encoding process, Secret S is any secret data that needs to be protected (e.g., secret encryption key).

Step –I: The fuzzy vault begins by concatenating 16-bits CRC data C from the initial secret S (56-bits key) to produce SC (72 bits). (This concatenation reduces the chance of a random error being undetected (i.e., failing to identify incorrect decoding)).

Step –II: SC is used to find the coefficients of the polynomial P: 72-bits SC can be represented as a polynomial with 8 (72/9) coefficients, with degree D=7, p(x) = c7x7 + c6x6 + ... + c1x + c0, by decomposing SC into non overlapping 9-bit segments, and each segment is declared as a specific coefficient ci, i = 0,1,2,..., 7.

Step –III: Find a set of ordered pairs G = {(x1, p(x1)), (x2, p(x2)), ...,(xN, p(xN))}, assuming that there are N unique template minutiae (x1, x2, ..., xN)

Step –IV: A second set of ordered pairs, called the chaff set C, is then generated from random x-coordinates c1,c2, ..., cM (distinct from x1,x2, ..., xN) such that C = {(c1,d1), (c2,d2), ...,(cM, dM)} and di = p(ci), ∀i. The union of these two sets G ∪ C is randomized to produce vault set VS.

Thereafter, a user tries to unlock the vault V using the query minutiae features.

Decoding: The decoding process can be described by Fig.5

Step-I: Given N query minutiae (Q) x1*, x2*, ..., xN*, the points to be used in polynomial reconstruction are found by comparing x1*, i =1,2,..... , N, with the abscissa values of the vault V, namely v1,l = 1, 2, ..., (M+N):

if any x1*, i=1,2, .........N is equal to vl = 1, 2, .... , (M+N), the corresponding vault point (vl, wl) is added to the list of points to be used. Assume that this list has K points, where K≤N.

Step-II: (For decoding a degree D polynomial, (D+1) unique projections are necessary). All possible combinations of (D+1) points, among the list with size K are considered, resulting in (k/D+1) combinations. For each of these combinations, the Lagrange interpolating polynomial is constructed. For a specific combination set given as L= {(v1,w1), (v2,w2), ...(vD+1, wD+1)}, the corresponding polynomial is yielding.

p*(x) = c7* x 7 + c6* x 6 + ... + c1* x + c0*. The coefficients are mapped back to the decoded secret SC*.

If the CRC remainder on SC* is not zero, it is certain that there are errors.

If the remainder is zero, with very high probability, there are no errors.

Step-III: SC* is segmented into two parts:

The first 56 bits denote S* while the remaining 16 bits are CRC data.

Finally, the system outputs S*. If the query minutiae list overlaps with the template minutiae list in at least (D+1) points, for some combinations, the correct secret will be decoded, namely, S* = S will be obtained.
This denotes the desired outcome when the query and template fingerprints are from the same finger.

Phase – III: Detection and Attack: The notations are as follows:

- \( D_i \): The database template corresponding to user \( i \), \( i = 1, 2, 3, ... , N \) where \( N \) is the total number of users registered in the system. It is assumed that the attacking system knows the format of this template, but it cannot access the template itself.
- \( n_i \): The total number of minutiae in \( D_i \). Note that the attacking system does not know this value.
- \( T_{ij} \): The \( j \)th synthetic template generated by the attacking system for user \( i \). This template has the same format as database templates; it can be represented as

\[
T_{ij} = \begin{bmatrix}
1_c^i & 1_r^i & 1_\theta^i \\
2_c^i & 2_r^i & 2_\theta^i \\
\vdots & \vdots & \vdots \\
{n_i}c^i & {n_i}r^i & {n_i}\theta^i
\end{bmatrix} \tag{1}
\]

Where each row represents column index, row index and orientation associated with a minutia; upper left hand subscript denotes the minutiae index, so the total number of minutiae in \( T_{ij} \) is \( n_j \).
- \( S(D_i, T_{ij}) \): The matching score between \( D_i \) and \( T_{ij} \).
- \( \text{St} \): The decision threshold used by the matcher. Note that the attacking system does not know this value.

For attacking a specific user’s account, the attacking system follows the following five steps:

1. **Step 1 (Initial guessing):** Generate a fixed number of synthetic templates. In the current implementation, 100 random minutia templates \( (T_1, T_2, T_3, ... , T_{100}) \) are created.
2. **Step 2 (Try initial guesses):** Attack user \( i \) account with the templates generated in Step 1; accumulate the corresponding matching scores \( (S(D_i, T_1), S(D_i, T_2), S(D_i, T_3),... , S(D_i, T_{100})) \).
3. **Step 3 (Pick the best initial guess):** Declare the best guess \( (T_{i}^{\text{best}}) \) to be the template resulting in the highest matching score. Declare the best score \( (S_{\text{best}}(D_i)) \) to be the highest matching score.
4. **Step 4 (Try modification set):** Modify \( T_{i}^{\text{best}} \) by (i) perturbing an existing minutia, (ii) adding a new minutia, (iii) replacing an existing minutia, and (iv) deleting an existing minutia. If for any one of these attempts, the matching score is larger than \( S_{\text{best}}(D_i) \), declare the modified template as \( T_{i}^{\text{best}} \), and update \( S_{\text{best}}(D_i) \) accordingly. Else, do not change the parameters of \( T_{i}^{\text{best}} \).
5. **Step 5 (Obtaining result):** If the current best score is accepted by the matcher (namely, \( S_{\text{best}}(D_i) > \text{St} \)) threshold, stop the attack; else, go to Step 4.

It is assumed that the resolution in dpi and size in pixels of the images generating the original templates is known to the attacking system. The sensor manufacturers announced these values.

The image size is used for generating the location of synthetic minutiae; the resolution determines the inter-ridge distance (9 pixels for 500 dpi) associated with the fingerprints. For eliminating the generation of minutiae too close to each other, first create a rectangular grid. Then, the 2D location of a minutia, \((c, r)\), is created to be in the center of those cells, where the cells to be occupied are selected randomly. Hence, the attacking program does not create minutiae that are closer than the inter-ridge distance. This helps in creating dispersed minutiae sets.

Phase IV: Authentication:

i. A sensor and some pre-processing functions, to capture the fingerprint impression from an individual as input data.
ii. A comparison process that evaluates the similarity between the stored reference templates and the captured data sample and that result in a similar score.
iii. A storage entity with the fingerprint impression samples of the enrolled individuals that is linked to or integrated in a database with the identity information of the corresponding individuals.
iv. A decision function that decides if a fingerprint sample matches to a certain reference template or not.

4. Conclusion

The basics of fingerprint biometric authentication system and its combination with crypto key generation methods to provide elevated security is presented in this paper. The methods and mechanisms for extracting minutiae points from input fingerprint images are discussed in detail, also architecture for designing a biometric cryptosystem through which a user can securely access and receive information only by using his fingerprint impressions is discussed, which is very efficient and effective mechanism to authenticate the legitimate users only by successful detection of a kind of attack named PARD attack.

5. Future Scope

This paper presents a secure authentication system which provides protection to the data by using bio-crypto system based on fuzzy vault. Through this mechanism this system can prevent the access of unauthorised users. The issue of prevention from those attacks can be handled
in future also work can be done in the direction to find better transformations used in the system for security, i.e., more discriminable fingerprint features can be designed to improve the security.

References


Biography

Indu Verma is working as an assistant professor in Ajay Kumar Garg Engineering College, Ghaziabad, U.P.(India), she has obtained her M-Tech (Computer Engineering) with Hons. from Shobhit University and MCA from U.P technical University, Lucknow (U.P). She has been in teaching from last 6 years; she has been member of several academic and administrative committees. During her teaching tenure she has also been coordinated a National Conference and many Technical fests at college level. She has attended several seminars, workshops and conferences at various levels. Also she has some papers published at national and international conferences. Her area of research includes Network Security and database.

Avimanyou Kumar Vatsa is working as Research Assistant and pursuing PhD at Department of Computer Science, University Of Missouri-Columbia, Columbia, MO, USA. He worked as Assistant Professor and Coordinator - CSE at Shobhit University, Meerut, (U.P), INDIA. He obtained his M-Tech (Computer Engineering) with Hons. from Shobhit University and B-Tech(I.T) from V.B.S. Purvanchal University, Jaunpur (U.P). He has worked as software engineer in software industry. He has been in teaching from more than one decade. He is on the editorial board and reviewers of several international and national journals in networks and security field. He has been member of several academic and administrative bodies. During his teaching he has been coordinated many Technical fests and National Conferences at Institute and University Level. He has attended several seminars, workshops and conferences at various levels. His many papers are published in various national, international journals and conferences. His area of research includes MANET (Mobile Ad-Hoc network), Network Security, Congestion Control and VOIP-SIP (Voice over IP).