Data Sharing And Rules Intersection In Cooperative Heterogeneous Network

P. Balanancy[*1], **S. Priyanka**[*2], **T. Vethavalli**[*3], **Mrs. S. Selvakanmani**[*4]

[1,2,3]UG Students, [4]Assistant Professor

Department of Computer Science and Engineering, Velammal Institute of Technology, Ponneri, Tiruvallur

Abstract - Data sharing between two independent networks is a difficult task in a connected network. The process of sharing data between two independent networks in term of breaking firewalls plays a major role. The rules that are available to cross out the firewalls are a difficult one. The systems that are in previous does not allow the node in it to break the network restriction so that the network reachability is not at a high one. The network restriction is reducing to make the data sharing to the node in the different network. The pairwise independent network model is a special case of the multi-terminal, where the pairwise source observed by every pair of terminals is independent of those sources observed by any other pairs. The data in the exist one are allow the data to be shared without any restriction in the data sharing. So, that the data communication lead into a unhealthy communication that in term lead to hacking process and intrusion process. The data communication should be an easy one so that data shared in easily. The data communication occur at the node side between two different network allow the user to share data across and make the network reachability.

Keywords: Heterogeneous network, Rules intersection, firewall, admin, database, file sharing.

I. INTRODUCTION

Network security: A combination of computer hardware, cabling, network devices, and computer software used together to allow computers to communicate with each other. The goal of any computer network is to allow multiple computers to communicate. The type of communication can be as varied as the type of conversations you might have throughout the course of a day. For example, the communication might be a download of an MP3 audio file for your MP3 player; using a web browser to check your instructor’s web page to see what assignments and tests might be coming up, checking the latest sports scores; using an instant-messaging service, such as AOL Instant Messenger (AIM), to send text messages to a friend; or writing an e-mail and sending it to a business associate. This chapter starts the process of closely looking at the four networking components mentioned in the formal definition: computer hardware, computer software, cabling, and networking devices. Before you look at each component, however, it is helpful to think about some examples of networks.

A Small Network: Two PCs and One Cable You can create a simple network with two computers and a cable. Although it’s not a terribly impressive network, such a network does occasionally serve a good purpose in real life, as well as being useful for discussing networking and learning some basic skills in classroom labs.

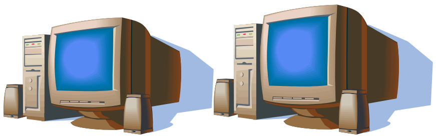


Fig 1:A Two-PC, One-Cable Network

There are many different computing and networking technologies — some available today, some just now emerging; some well-proven, some quite experimental. Understanding and solving today's computing dilemma more completely involves recognizing technologies; especially since a single technology by itself seldom suffices and, instead, multiple technologies are usually necessary.

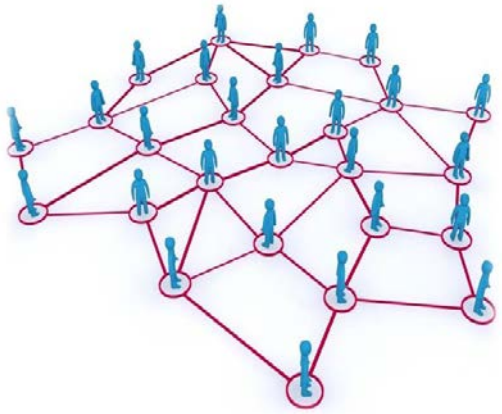


Fig 2: Network image

Some technologies are being obsoleted, some are maturing, some are adequate, and some are vital. A single and simple frame of reference is most helpful in understanding the concepts of individual networking technologies, seeing how they operate, and recognizing relationships among technologies. The various technologies share many fundamental concepts. This chapter provides an introduction to the world of networking technologies. It establishes a much generalized reference model, and then classifies technologies into categories relative to this model. A complete and generalized computing reference model is quite helpful in describing different technologies and their relationships. Many different groups in the computing industry have been involved during the last decade in developing computing reference models — some models for operating systems, some for data bases, some for application systems, and some for communications networking — but only recently have efforts begun in earnest to combine these various models into a single, more complete, but yet simpler reference model. Such a generalized model can be based easily upon established networking models Application Support has two divisions, called the Application Programming Interface (abbreviated API-A for a particular application 'A'), and Application Support (abbreviated SUPP-A). The API and the application support are closely tied together, and are chosen by the application programmer based upon the requirements of the application. Examples of application programming interfaces include CPI-C (Common Programming Interface for Communications), RPC (Remote Procedure Call), and MQI (Message Queue Interface). Depending upon the API selected, the application services may be quite different. For instance, CPI-C utilizes Advanced Program-to-Program Communication (APPC) and SNA logical unit 6.2 (LU 6.2) services, which includes the protocol flows between two applications for establishing a conversation, exchanging data, ensuring commitment of resources, and terminating a conversation. RPC does networking through program stubs that are customized for each application program and then attached (linked). RPC usually operates over TCP/IP protocols. MQI provides queue-to-queue communication, in lieu of direct program-to-program communication over a dedicated logical connection; it is a form of networking middleware with resource commitment and assured message delivery. MQI operates over LU 6.2, TCP/IP, and other networking protocols. Transport Network, which corresponds to the critical Transport and Network OSI layers, is abbreviated TPORT-A for a particular application 'A.' These two layers work closely together to ensure that user data is transmitted with a predictable level of service from the source node to an end node, perhaps through a set of intermediate nodes. Depending upon the specific protocol chosen, these layers provide such functions as optimal route determination, error detection and recovery, and congestion control. Examples of transport protocols include TCP/IP and SNA Advanced Peer-to-Peer Networking (APPN*). Each of these protocols utilizes unique addressing structures, protocol flows between peer transport layers in end nodes, and routing protocols between intermediate nodes. Please note that throughout this book the term “transport protocol” will refer to the combination of these two OSI layers (unless explicitly identified as OSI layer to match nomenclature commonly used in the industry. Also note that, historically, the Application Support and Transport Network have been very closely tied together and the selection of a particular API forced the selection of a particular network protocol, or, conversely, a programmer was forced to select an API based on the currently supported transport protocol in the network. For instance, Remote Procedure Call (RPC) and the TCP sockets interface are closely associated with the TCP/IP transport protocol, and would be the application programming interface of choice for a TCP/IP-based transport network; however, if a CPI-C-based application might solve a particular business requirement, then SNA transport would have to be added to this TCP/IP network to support the CPI-C-based application, which might involve substantial effort. Sub networking, abbreviated SNETG corresponds to the OSI Data Link Control and Physical layers. These layers are concerned with getting data on the physical media of the network, and then getting it reliably and efficiently from one physical node to the next physical node in the network.

The fundamental concepts necessary for an easy discussion of available and emerging techniques are:

- Stacks of software
- Switching points
- Model layers (or software program groups)
- Application (APPL)
- Application Support (SUPP)
- Networking (NETG)
- Transport Network (TPORT)
- Sub networking (SNETG)

The one network component that has not yet been covered in this chapter is software. Software provides the motivation and the reasons why a computer tries to communicate in the first place. You might build a network with computer hardware, NICs, modems, cables, and networking devices, but if no software exists, the computers do not attempt to communicate. Software provides that logic and that motivation for a computer to communicate. You might have used computer software that, in turn, caused the computer to use the network. If you have ever opened a web browser to look at web pages or surf the web, you have used computer software that drives traffic across the network.

II. EXISTING SYSTEM

The process of forwarding data between two independent network is a difficult task. To overcome that type of issue this system allow the data to forward in an easy way. The easy way is provided to the user in term of reducing the network security way. The system work on it to reduce the firewall way so that the data forwarding will be easy one. Alice and Bob wish to generate a secret key (SK) and a private key (PK) simultaneously, with the help of two external relays[2]. The SK needs to be protected from Eve that has access to the public discussion [4], whereas the PK needs to be protected from Eve and the two relays. The motivation for using this model is that the two terminals may need to agree on several keys, with different security clearance levels in the presence of eavesdroppers in practical systems[6]. For instance, in tactical networks or wireless networks for the financial industry, Alice and Bob may wish to simultaneously exchange two types of data with different security constraints, where one type of data with a lower security constraint can be revealed to the licensed users in these networks[7]-[11], but the other type of data with a higher security constraint is not allowed. Correspondingly, two types of keys with different security clearance levels are required.

A. Disadvantages

✓ The data sharing occur without any security

✓ The authorized data can be shared to the node belong to other network.

✓ The rule freelance increase the hacking process

✓ The independent network in dependency get break out because the rules are break out

✓ The rules of each network are explicit to other network cause network crash.

B. Problem Definition:

The major issue in forwarding data at physical layer from one node to another is establishing connection over the nodes. If the connection enabled making use of trusted relay will be good in one to one communication which slow the down the efficiency of the communication because the communication will occur between one to one node at a time.

III. PROPOSED SYSTEM

The proposed system work on sharing of data between two independent network. The data should occur in a secured way so that the data reachable occur in a network is achieved. The data sharing in the network start with the independent network. Then the process extend to the data sharing via the IP address of the particular node in the other independent network. The data forwarding between the networks occur in term of forwarding the data to the network by breaking out the firewall in a secure way. The admin who were allowing the data communication between the network look for data transmission. The data first get forwarded to the admin of the independent network the admin check for the data that going to transferred to the next node available in the other network. The data get monitored by the admin at the time of data getting forwarded. The data only get forwarded to the user only through the admin alone. The data forwarding occur in term of admin of the independent network and the in term of admin connecting the two independent network.

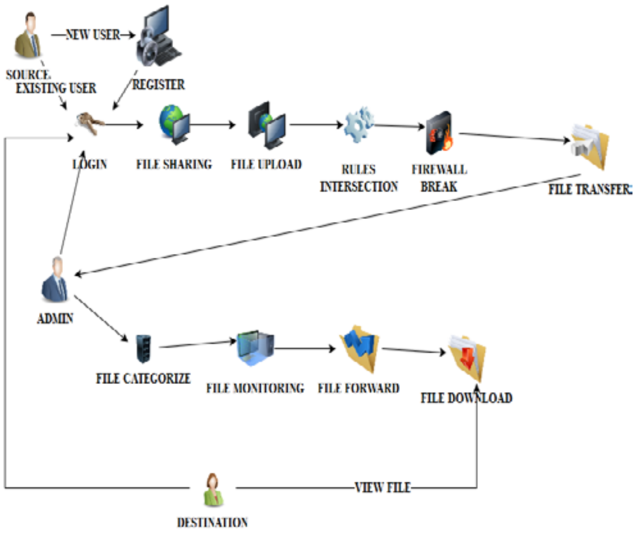


Fig 3: Architecture diagram

The admin get the rules of both network first. Then the intersection process on the rules is performed. After performing the rules intersection the set of rules that is availed to break the fire wall is provided to both the user. The user just make use of the rule intersection to break the rules then the data get forwarded from one node to another

This Architecture diagram denotes the process of data sharing between independent networks. The user belongs to heterogeneous network register their details along with IP address and port number and login in to it. If the user is already registered, they can login directly. Login details are maintained by admin. In this process, Secret Key-Private Key algorithm is used to access and transfer the data. After, login sender wants to share the file to receiver. Then file sharing and file uploading process monitored by admin. Secret key is generated to access and upload the file without any corruption. Then rules intersection occurred between independent networks through admin. Rules intersection is the process of connecting the common rules between both nodes. Each node has the different rules and that is explicitly identified which nodes are ready to share the files. Here the rule's intersection process breaks the firewall to transfer the file to the receiver. This file transfer done by using the private key. The receiver side admin check whether the incoming file is authorized file or not. It categorizes the file and monitor that process of file sharing. Also, it checks the IP address and port number of the destination node and then forward the file to it. Once receiver gets the file then file downloading process occur. Finally, receiver can view the file and send the acknowledgement to the sender.

A. Objective and Scope

Objective of the project is to avoid the polluted data that get to added to the original data when it get forwarded to destination from source through intermediate nodes the data will get scanned or filtered using median filtering technique. Scope of the project is when the data get forwarded from source to destination will be forwarded as text content to avoid or to overcome the excess of polluted data added to it. The image file get converted to text file in term of extracting the binary value of the image file.

B. SK-PK Generation Algorithm

The first cooperative SK-PK generation algorithm is proposed based on the careful combination of the point-to-point pairwise key generation technique, application of the onetime pad and the XOR operation. Specifically, three main steps are considered:

1) every pair of the four terminals agrees on a pairwise key using their correlative observations;

2) the two relays help Alice and Bob to share additional CR based on repeated application of the one-time pad over the public channel;

3) the total CR shared by Alice and Bob is divided into two parts: one part is agreed on as the expected SK, whereas the other part is converted to the expected PK using the XOR operation.

C. Pseudo Code

Algorithm: The First Algorithm for the PIN

Step 1: Pairwise key agreement:

Based on Slepian-Wolf coding, every pair of the four terminals agrees on a pairwise key using their correlated source observations. In particular, Alice (Bob) and relay i

agree on a pairwise key $WA;i$ ($WB;i$), i = 1, 2; the two relays agree on $W1;2$; Alice and Bob agree on $WA;B$.

Step 2: Generation of additional CR:

- For each i = 1, 2, divide the pairwise keys as: $WA;i$ =($W1 A;i$,$W2 A;i$), $WB;i$ =($W1B;i$,$W2B;i$).

- Each relay i sends $W1A;i \oplus W1B;i$ over the public channel, so that Alice and Bob can agree on the common message Wi , $WA;i$ since they know either $W1$

$A;i$ or $W1B ;i$.

- Then, the two relays help Alice and Bob to share one more common message ~$W1;2$, utilizing application of the one-time pad with respect to the pairwise keys

($W2A;1$,$W2B;1$,$W2A;2$,$W2B;2$,$W1;2$) as shown in Fig. 2.

Step 3: SK and PK agreement:

- Now, for the CR ($WA;B$,$W1$,$W2$, ~$W1;2$) shared between Alice and Bob in the previous two steps, let $WA;B$ = ($KS;3$,$KP;3$), Wi = ($KS;i$,$KP;i$),

i = 1, 2.

- Alice and Bob agree on KS , ($KS;1$,$KS;2$,$KS;3$, ~$W1;2$)

as the final SK, and KP , ($KP;3$,$KP;1 \oplus KP;2$) as the final PK.

IV. MODEL

Two terminals, Alice (A) and Bob (B), wish to agree on a key through a wireless fading channel in the presence of an ac-tive attacker Eve (E). All three terminals can transmit over the wireless channel. We assume that Alice and Bob are half-duplex nodes, while the attacker is a full-duplex node. In this paper, we assume that the goal of the attacker is to minimize the key rate generated by Alice and Bob from the wireless channel. The at-tacker can receive a noisy version of the signal transmitted by the legitimate terminals. In addition, it can transmit signals to contaminate the signal transmitted by the legitimate users. In particular, if Alice transmits X_A in a given channel use, then Bob and Eve receive

$$Y_B = h_{AB}X_A + X_{E1} + N_B \qquad (1)$$

And $$Y_E = h_{XA}X_A + N_E \qquad (2)$$

respectively, in which h_{AB} is the channel gain from Alice to Bob, X_{E1} is the signal transmitted by Eve and received by Bob, N_B is zero mean Gaussian noise with variance σ^2, h_{AE} is the channel gain from Alice to Eve, and N_E is zero mean Gaussian noise with variance σ^2 . We note that what matters from the at-tacker's perspective is the signal that arrives at the legit-imate receiver. In this paper, we assume that the eavesdropper knows its channel state to the legitimate receiver and can hence control its output signal X_{E1} to the legitimate receiver to achieve its attacking goal by mitigating the impact of its channel on the output signal. Hence, we did not assume any particular fading model from the attacker and legitimate receiver. In the following, we will characterize the optimal distribution of the optimal arriving attack signal. Alternatively, if Bob transmits X_B in a given channel use, then Alice and Eve receive

$$Y_A = h_{BA}X_B + X_{E2} + N_A \qquad (3)$$

$$\text{And} \quad Y_E = h_{XB}X_B + N_E \qquad (4)$$

respectively, in which h_{BA} is the channel gain from Bob to Alice, N_A is zero mean Gaussian noise with variance σ^2 and h_{BE} is the channel gain from Bob to Eve. We note that the anal-ysis can be easily carried out to the case in which the noise variance σ^2 of N_A is different from that of N_B. Similarly to (1), X_{E2} is the attack signal from the attacker as received by Alice. We assume that N_A, N_B and N_E are independent of each other. We note that in the model considered in [4]–[6],$Y_B = X_{E1,}$ and $Y_A = X_{E2}$ (i.e., if there is an active attack, the receiver receives a signal only from the attacker). We assume that the channel is reciprocal, that is $h_{AB} = h_{BA}$.Due to different transmission paths h_{AB}, is independent of h_{AE} and h_{BE} . We consider an ergodic block fading model, in which the channel gains arefixed for a block of T symbols and change to other values at the beginning of the next block. In this paper, we assume $h_{AB} \sim \mathcal{N}(0,\sigma^2{}_{h)}$ and $h_{AE} \sim \mathcal{N}(0,\sigma^2{}_{AE)}$.We assume that none of the terminals knows the value of the fading gains. The noise processes are assumed to be independent and identically distributed (i.i.d.) over channel uses and terminals. We also assume that Alice and Bob know the statistics of h_{AE} and $h_{BE.}$

Let $\mathbf{X}_A = [X_A(1),\ldots,X_A(N)]^T$ and $\mathbf{X}_B = [X_B(1),\ldots,X_B(N)]^T$ denote codewords sent by Aliceand Bob, respectively, and X_E be the attack signalsent by Eve (which results in the received signals X_{E1} and X_{E2})over N uses of the channel. Here,N couldbe larger than the channel coherence time T,that is,a codeword can span multiple coherence blocks. Let $\mathbf{Y}_A = [Y_A(1),\ldots,Y_A(N)]^T$,$\mathbf{Y}_B = [Y_B(1),\ldots,Y_B(N)]^Tand\mathbf{Y}_E = [Y_E(1),\ldots,Y_E(N)]^T$ denote corresponding ob-servations at Alice, Bob and Eve, respectively. Since we havea half-duplex constraint on the legitimate users, $Y_A(i) = (\varphi)$when $X_A(i) \neq (\varphi)$. Here,φ denotes either no observationorno transmission. Similarly,$Y_B(i) = \varphi$ when $X_B(i) \neq (\varphi)$.To make a fair comparison to schemes in which only one terminal transmits, we have a total power con straint, that is

$$1/N\ E\{\mathbf{X}^T{}_A\,\mathbf{X}_A + \mathbf{X}^T{}_B\ \mathbf{X}_B\} <= P \qquad (5)$$

We also assume that the attacker has an average power con-straint ,that is

$$1/N\ E\{\mathbf{X}^T{}_E\,\mathbf{X}_E\} <= P_E \qquad (6)$$

Both Alice and Bob will generate a key based on the sequenceit sends and signals it receives from the wireless channel. Let f_A and f_B denote the key generation functions at Alice andBob, respectively, so that $K_{A=}f_A(\mathbf{X}_{A,}\mathbf{Y}_{A)}$ and $K_{B=}f_B(\mathbf{X}_{B,}\mathbf{Y}_B)$ .A keyrate **Rkey** is said to be achievable if for each €>0 , there exists an n_0 such that for each $N >= n_0$ we have that

$$P_r(K_A \neq K_B) <= € \qquad (7)$$

$$1/N\ H(K_A) >= R_{key} - € \qquad (8)$$

$$1/N\ I(K_A;\mathbf{Y_E},\mathbf{X}_E) <= € \qquad (9)$$

$$H(K_{A)} >= \log|K_A| - € \qquad (10)$$

in which$|K_A|$ denotes the size of the alphabet used for the dis-crete variable $K_{A.}$

A. Joint Source_Channel Key Agreement Protocol

In this section, we develop a joint source-channel key agree-ment protocol. Here, we assume that the eavesdropper is pas-sive, i.e., $X_E = 0$.Wefirst consider a scenario in which there exists a public channel, through which both Alice and Bob can exchange messages. All messages transmitted over the public channel will be overheard by Eve noiselessly. The scheme de-veloped in this scenario provides insight for a more realistic scenario in which there is no public channel available [8]-[10]. We then consider this more realistic model. In both cases, key agreement schemes that benefit from both the source model and the channel model are developed. In both scenarios, asymptotic analyses suggest that the channel model is asymptotically optimal as the coherence time of the channel becomes long. On the other hand, in the high power regime, the source model is asymptotically optimal. We also find that, in the asymptotic regime, either in long coherence time or high power, the achievable key rate without the public channel is the same as that we can achieve when there is a public channel.

B. Advantages

- ✓ The rules of independent network maintained secretly.
- ✓ The rules intersection is done by admin alone
- ✓ The rules does not explicit-ed to the node belonging to different network
- ✓ The rules intersection done at the time of data forwarding only
- ✓ The nodes doesn't know the original IP of the other node in the independent network.

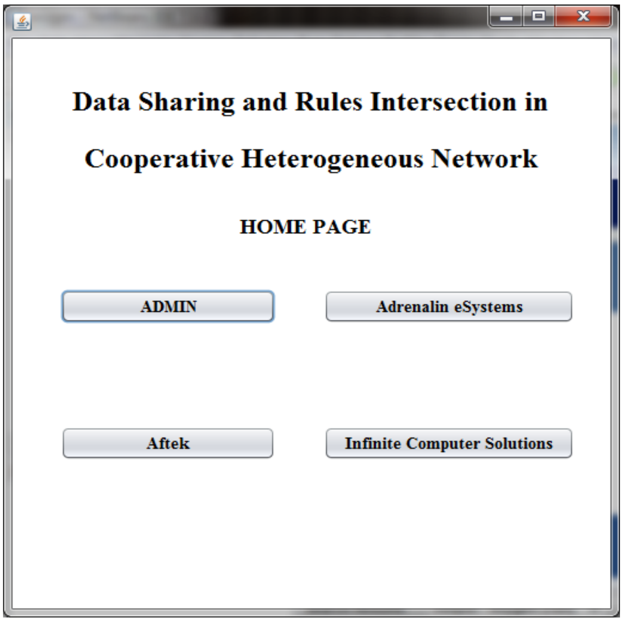
V. MODULES AND MODULE

Description

- ✓ Node Initialization and Rules Intersection
- ✓ Data forward and Firewall Break
- ✓ Data process and Network Reachability

A. Node Initialization and Rules Intersection

Node generation is a process of authenticating a node who were looking for a connection in that particular network. The log-in request get forwarded to the concern server of the internal network. To enable the node generation the user need to send their details to the server through registration process which help them to get an access control in that internal network. The internal network usually checks for authorized user then only enable the node to get access on the network. The node initialization process will get worked after the node get generated by the server. The server view the details provided by the user who were requesting for node generation in that particular internal network. Once verifying the details submitted by the user the node get generated in the network by the server. After node generation the particular user get access for that internal which it request. The node initialization process is done to make the node to involve for data uploading, data sharing, data securing, data forwarding in that internal network. Node generation is a process of authenticating a node who were looking for a connection in that particular network. The log-in request get forwarded to the concern server of the internal network. To enable the node generation the user need to send their details to the server through registration process which help them to get an access control in that internal network. The internal network usually check for authorized user then only enables the node to get access on the network. The node initialization process will get worked after the node get generated by the server. The server view the details provided by the user who were requesting for node generation in that particular internal network. Once verifying the details submitted by the user the node get generated in the network by the server. After node generation the particular user get access for that internal which it request. The node initialization process is done to make the node to involve for data uploading, data sharing, data securing, data forwarding in that internal network.

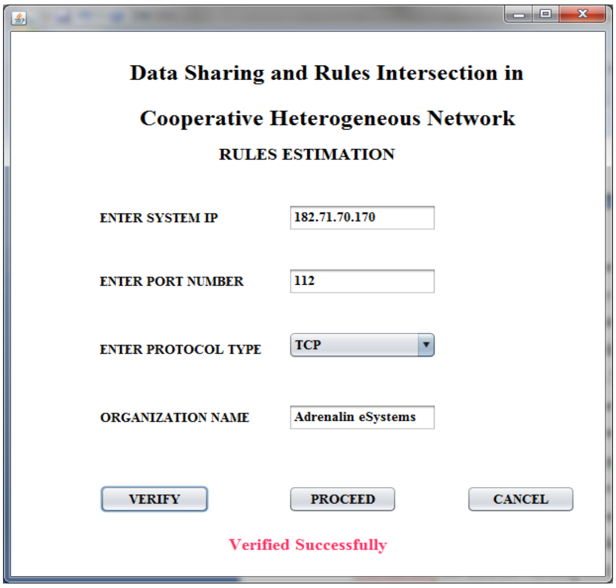


Data Sharing and Rules Intersection in

Cooperative Heterogeneous Network

HOME PAGE

Fig 4: Home page



Data Sharing and Rules Intersection in

Cooperative Heterogeneous Network

RULES ESTIMATION

ENTER SYSTEM IP 182.71.70.170

ENTER PORT NUMBER 112

ENTER PROTOCOL TYPE TCP

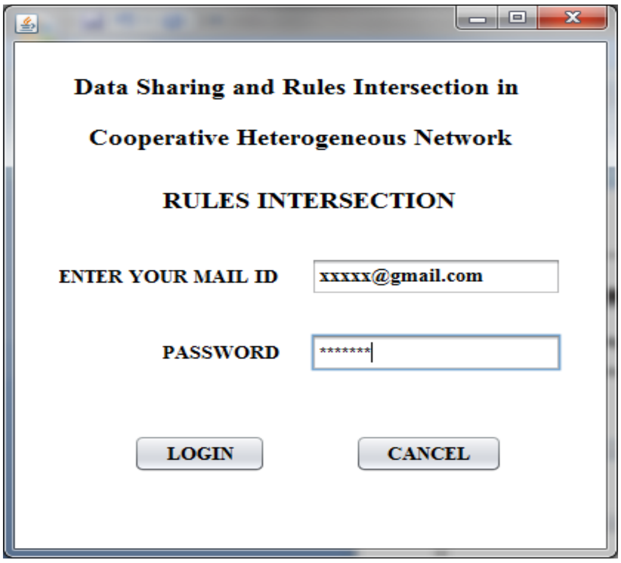
ORGANIZATION NAME Adrenalin eSystems

Verified Successfully

Fig 5: Node Initialization

B. Data Forward and Firewall Break

Data forward is process of forwarding the data to the node from one to another that are belongs to different networks. The network at the one node request the admin for data forward. Once the request get accepted by the admin the data forwarding process occur. The data at the node which is one network cross out the rules that are restriction of data forwarding. The data get forwarded to the node once the node forwarded the data to the admin. The admin check for the data that get forwarded to it. After the verification of the data the data get forwarded to the node of another network.



Data Sharing and Rules Intersection in

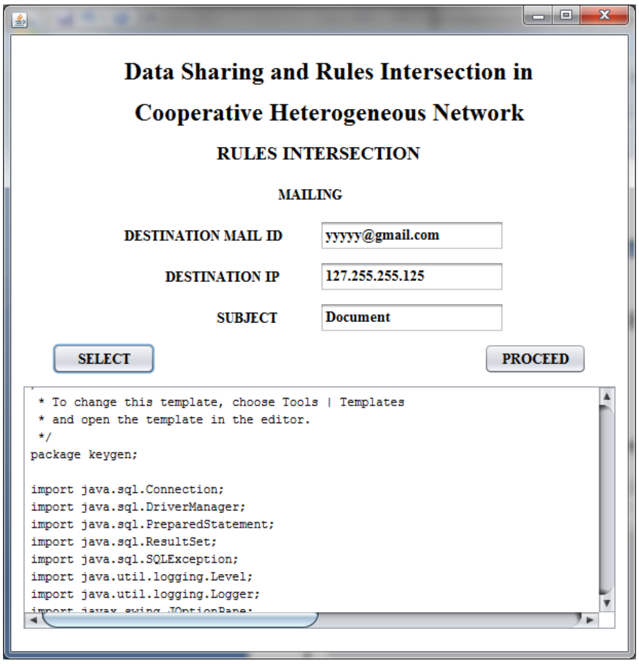
Cooperative Heterogeneous Network

RULES INTERSECTION

ENTER YOUR MAIL ID: xxxxx@gmail.com

PASSWORD: *******

Fig 6: Rules Intersection



Data Sharing and Rules Intersection in

Cooperative Heterogeneous Network

RULES INTERSECTION

MAILING

DESTINATION MAIL ID: yyyyy@gmail.com

DESTINATION IP: 127.255.255.125

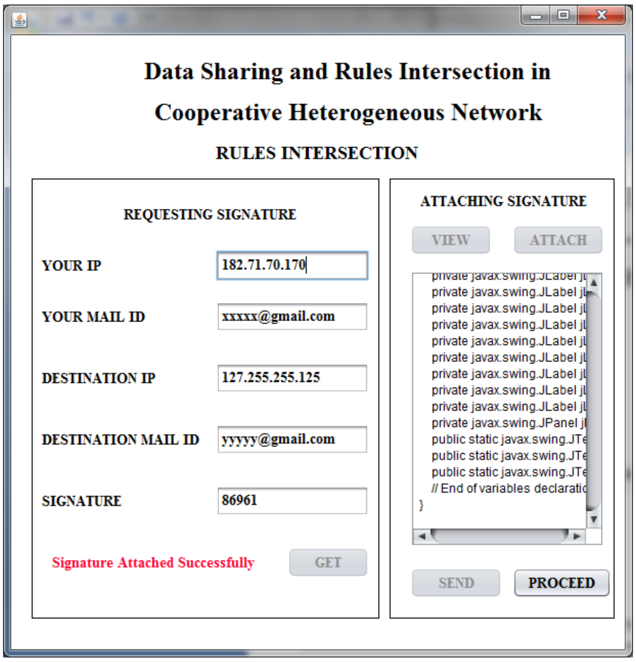
SUBJECT: Document

```
 * To change this template, choose Tools | Templates
 * and open the template in the editor.
 */
package keygen;

import java.sql.Connection;
import java.sql.DriverManager;
import java.sql.PreparedStatement;
import java.sql.ResultSet;
import java.sql.SQLException;
import java.util.logging.Level;
import java.util.logging.Logger;
import javax.swing.JOptionPane;
```

Fig 7: Data Forward

A firewall is a network security system, either hardware- or software-based, that uses rules to control incoming and outgoing network traffic. A firewall acts as a barrier between a trusted network and and an untrusted network. A firewall controls access to the resources of a network through a positive control model. This means that the only traffic allowed onto the network is defined in the firewall policy; all other traffic is denied. Firewall break done by the node in the independent network with the help of admin. The admin after of the intersection of the rules the rules get forwarded to the nodes who were looking for data forward to the different nodes available in the different network. The firewall get break by applying the rules implemented by the admin in term of firewall break. The firewall break done in a secure way to avoid data leakage. The data leakage occur when the data get transferred to the node which are belongs to different network. The data sharing in the network start with the independent network. Then the process extend to the data sharing via the IP address of the particular node in the other independent network. The data forwarding between the networks occur in term of forwarding the data to the network by breaking out the firewall in a secure way.



Data Sharing and Rules Intersection in

Cooperative Heterogeneous Network

RULES INTERSECTION

REQUESTING SIGNATURE

YOUR IP: 182.71.70.170

YOUR MAIL ID: xxxxx@gmail.com

DESTINATION IP: 127.255.255.125

DESTINATION MAIL ID: yyyyy@gmail.com

SIGNATURE: 86961

Signature Attached Successfully

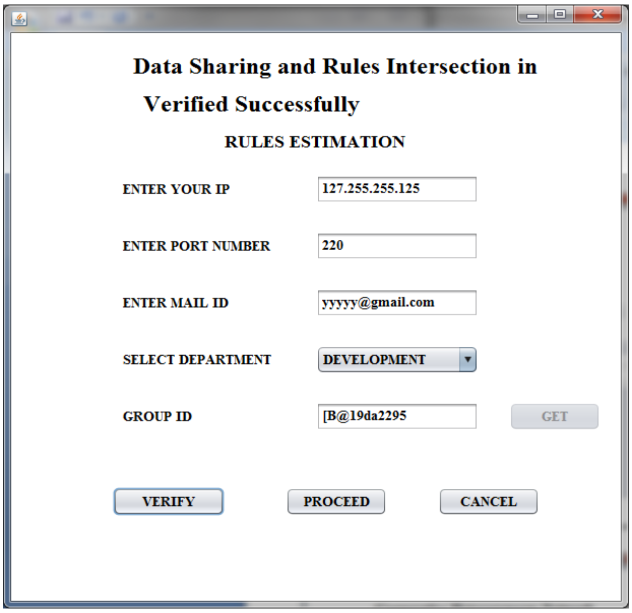
ATTACHING SIGNATURE

```
    private javax.swing.JLabel j
    private javax.swing.JLabel jL
    private javax.swing.JLabel jL
    private javax.swing.JLabel jL
    private javax.swing.JLabel jL
    private javax.swing.JLabel jL
    private javax.swing.JLabel jL
    private javax.swing.JLabel jL
    private javax.swing.JLabel jL
    private javax.swing.JPanel jP
    public static javax.swing.JTe
    public static javax.swing.JTe
    public static javax.swing.JTe
    // End of variables declaratio
}
```

Fig 8: Firewall Break

C. Data Process and Network Reachability

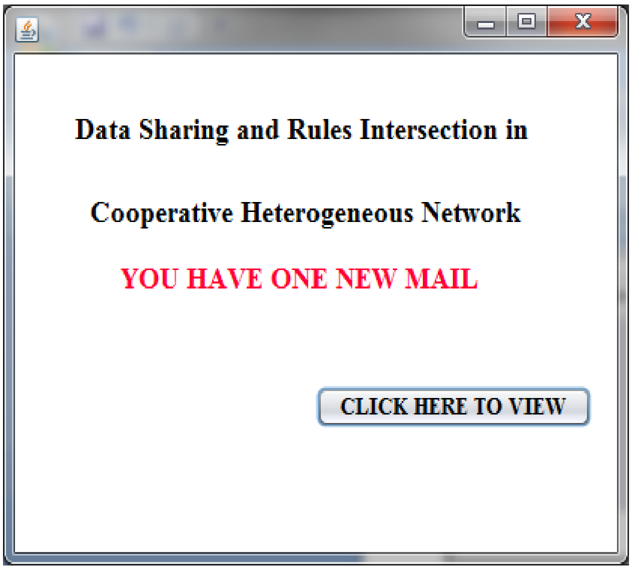
Data process is way of forwarding the data to the other independent network from one independent network. The independent network look for data forwarding between the network will because it an easy one. But forwarding the data to different network in term if the network is independent is difficult task. The data need to shared in a secure way so the data hacking is avoid. The firewall break done in a secure way to avoid data leakage. The data leakage occur when the data get transferred to the node which are belongs to different network. The process is way in which the data forwarding is generated by the admin who is monitoring both the network in term of data forwarding. The process of network reachable is done only if the data get forwarded between the nodes of two independent network in term of data leakage avoidance. . The data get monitored by the admin at the time of data getting forwarded. The data only get forwarded to the user only through the admin alone. The data forwarding occur in term of admin of the independent network and the in term of admin connecting the two independent network. The data get forwarded to the different network without any difficult lead to network reachability for data forwarding and processing. The data forwarding done through admin monitoring lead to forward and secure data forwarding between independent networks.



Data Sharing and Rules Intersection in
Verified Successfully
RULES ESTIMATION

ENTER YOUR IP	127.255.255.125
ENTER PORT NUMBER	220
ENTER MAIL ID	yyyyy@gmail.com
SELECT DEPARTMENT	DEVELOPMENT
GROUP ID	[B@19da2295

Fig 9: Data Process



Data Sharing and Rules Intersection in

Cooperative Heterogeneous Network

YOU HAVE ONE NEW MAIL

Fig 10: Network Reachability

VI. CONCLUSION

The process of transferring the data in a secured way without any destruct to the data in term of while it getting forwarded through intermediate nodes like wise the system is designed. The system not only check for hacking process happen or not it also check for not to hacking process to held while forwarding the data. The system work starts from the forward the data upload, continues on data share and withstand until the download of data at the destination side.

VII. REFERENCES

[1] "Simultaneously Generating Secret and Private Keys in a Cooperative Pairwise Independent Network" Peng Xu, Zhiguo Ding, Senior Member, IEEE, Xuchu Dai and George K. Karagiannidis, Fellow, IEEE Transactions on Information Theory,2016.

[2] J. Wang, J. Lee, F. Wang, and T. Q. S. Quek, "Jamming-aided secure communication in massive MIMO Rician channels," IEEE Trans. Wireless Commun., Dec. 2015.

[3] S. H. Chae, W. Choi, J. H. Lee, and T. Q. S. Quek, "Enhanced secrecy in stochastic wireless networks: Artificial noise with secrecy protected zone," IEEE Trans. Info. Forensics and Sec., vol. 9, no. 10, pp. 1617–1628, Oct. 2014.

[4] M. Z. Win, A. Rabbachin, J. Lee, and A. Conti, "Cognitive network secrecy with interference engineering," IEEE Netw., vol. 28, no. 5, pp. 86–90, Sep. 2014.

[5] A. Mukherjee, S. Fakoorian, J. Huang, and A. Swindlehurst, "Principles of physical layer security in multiuser wireless networks: A survey," IEEE Commun. Surveys Tutorials, vol. 16, no. 1, pp. 1–24, Feb. 2014. 10.1109/TWC.2015.2491935, IEEE Transactions on Wireless Communications.

[6] L. Wang, M. Elkashlan, J. Huang, N. H. Tran, and T. Q. Duong, "Secure transmission with optimal power allocation in untrusted relay no. 3, pp. 289–292, Jun. 2014.

[7] V. N. Q. Bao, N. Linh-Trung, and M. Debbah, "Relay selection schemes for dual-hop networks under security constraints with multiple eavesdroppers," IEEE Trans. Wireless Commun., vol. 12, no. 12, pp. 6076–6085, Dec. 2013.

[8] J. Lee, A. Conti, A. Rabbachin, and M. Win, "Distributed network secrecy," IEEE Journal on Sel. Areas in Commun., vol. 31, no. 9, pp. 1889–1900, Sep. 2013.

[9] R. Zhang, L. Song, Z. Han, and B. Jiao, "Physical layer security for two-way untrusted relaying with friendly jammers," IEEE Trans. Veh. Techn., vol. 61, no. 8, pp. 3693–3704, Oct. 2012.

[10] K. Ren, H. Su, and Q. Wang, "Secret key generation exploiting channel characteristics in wireless communications," IEEE Wireless Commun., vol. 18, no. 4, pp. 6–12, Aug. 2011.

[11] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, and N. B. Mandayam, "Information-theoretically secret key generation for fading wireless channels," IEEE Trans. Inform. Forensics and Sec., vol. 5, no. 2, pp.