ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Performance Analysis of Scheduling and Dropping Policies in Vehicular Delay-Tolerant Networks

Gajanand Sariyam[1], Priyanka Bhadoria[2,]

Lecturer, Dept. of Electronics and Telecommunication, Government Women's Polytechnic College Jabalpur, India[1]

Lecturer, Dept. of Computer Science, Kalaniketan Polytechnic College, Jabalpur, India [2]

ABSTRACT: According to the delay-tolerant-network (DTN) model, the DTN model is gaining traction as a practical communications platform over the old approach. Latency-tolerant networking (DTN) is a method to help to manage and deal with potential network outages that may occur due to delayed or lost connectivity, prolonged or changeable delay, uneven data rates, and high error rates in network setups with disparate elements. DTN's top priority has been dealing with security issues. DTNs result in unsecure data transfers because of the unsuitable security solutions. The proposed solution includes a malware detection system and security for each packet or bundle (including malware packets or bundles) that is sent over the network.

KEYWORDS: Bundle Security Protocol, Delay Tolerant Networks, Digital Signature, E Top-and-Tail Virus Scanning,

I. INTRODUCTION

Latency-tolerant networking (DTN) is a technology designed to deal with the variability in connectivity, extended delay, and high error rates in heterogeneous networks. For extreme settings or in space, examples of these kinds of networks include: DTN's top priority has been dealing with security issues.

DTNs result in unsecure data transfers because of the unsuitable security solutions. When a network is compromised by a virus, the data transit between network nodes is vulnerable to such issues as confidentiality, integrity, and availability. An attack on the availability of data across nodes is called denial of service. Another form of this type of assault is the Man-in-the-Middle attack in which an attacker can either intercept or manipulate the data packets, as they are being sent between network nodes.

A pioneer researcher on computer viruses, Fred Cohen, described a computer virus as a programme that is capable of replicating and evolving into other programmes. Figure 1 illustrates Dr. Cohen's rudimentary computer virus as pseudo-code. Computer viruses frequently use this type of three-subroutine structure. The first subroutine, the executable infector, is in charge of locating all the executable files on the system and infecting them by inserting the code from the infectious executable into them. do-damage is the malicious portion of the virus's payload. This final subroutine is known as a trigger-pulled check, and its responsibility is to ensure that the conditions above are met in order to deploy its payload.

There are unique security issues posed by a virus that is built on the DTN model, which is not found in traditional infrastructure. The central cellular carrier in the infrastructure model keeps an eye on the networks to see if there are any problems. We cannot guarantee if the data being transmitted between the nodes has arrived at its destination or has been secured. we provide a multidisciplinary approach for strengthening Delay Tolerant Networks, such as Top-and-Tail virus detection and the Bundle Security Protocol.

You can find simple ways to find out if your computer has a virus. The majority of techniques look for predetermined sequences of bytes known as strings. For a speedier virus detection, scanning only the first and last 2, 4, or 8 KB of a file for each potential position is an effective method. This proposed strategy is termed top-and-tail scanning, and it is employed in the technique to optimise scanning speed by lowering the number of disc reads. As the bulk of early computer viruses attached, appended, or replaced the target objects, top-and-tail scanning caught on as a standard practise.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

Protocol Specification includes:

1. Bundle-A bundle is a protocol data unit of the DTN bundle security protocol.
2. Bundle payload - A bundle payload (or simply "payload") is the application data of a file.
3. Fragment - A fragment is a bundle in which payload block contains fragments of payload.
4. Bundle node - A bundle node (simply a "node") is any end machine that can send and/or receive bundles.
5. Deletion, Discarding - A Bundle Security Protocol "discards" a bundle by simply ceasing all operations on the bundle and functionally erasing all references to it.

II. RELATED WORK

In order to defend the reactive routing Protocol against attackers and improve network performance, Pirzada et al.[3] created a "reputation system in MANETS." The examination of those safe routing protocols for MANETs shows that these protocols either build trust values between nodes using the watchdog mechanism or ACK messages. In MANETs, either direct or indirect measures can evaluate one node. Direct measured by means of the monitoring system or the ACK from the destination. "Reputation values built with ACK messages sent by target nodes" proposed by Keyun Liu and Jing Deng[4]. For the following reasons, these strategies are not applicable to DTNs. In DTNs, the watchdog process cannot be used and an intermediate knot monitored once its packets are forwarded to it. This is due to the absence of linkages on an end-to-end path at the same time, and hence an intermediate node must save, carry, and wait for transfers. The node loses connection with the intermediate node to be monitored. The 'working on the application of reputation systems in P2P networks' were offered by K. Aberer and Z. Despotovic [5] However, DTNs are not subject to reputations for P2P networks otherwise it will take too long to develop the values of peers' reputation. The idea that a peer can monitor others and get direct observations or a peer can investigate the reputational worth of another peer (and so receive indirect observations) before using the services offered by that Peer is most commonly suggested by P2P reputational management techniques. Neither of them is practical for DTNs, though. As we explained earlier, direct observations in DTNs are not possible. In addition, investigations into the reputation worth of an individual in DTNs are not practicable due to occasional communication in contact periods and intermittent peers' connectivity. "Challenges of safe co-mune communication in DTNs," suggested Vellambi and F. Fekri[6]. Here is advised the usage of identity-based encryption (IBC). IBC provides both source authentication, anonymous communication and confidentiality. It is proposed to increase message transmission rates by using packet replication rather than by means of cryptographic algorithms. They remark that existing DTN secure techniques only enable privacy and authentication of the data. Jing Su et al. [7] proposed a "Efficient countermeasure to infect Bluetooth worms" to prevent the device from being discovered or even turn off Bluetooth radio. You cannot find this approach attractive: devices can ban legit applications from using Bluetooth. Although Bluetooth worms are spreading orders of magnitude more slowly than the Internet worms, Bluetooth worms can spread swiftly enough to make it impossible to execute human-mediated counter-response methods in practise. These solutions must identify the presence of a worm, analyse infected code, and generate, test and deploy a safety patch within several days based on their simulations.

III. PROPOSED SYSTEM

Though the previous papers written for securing the DTN was secured with IBC [9], there are of course some more security issues in a DTN. They are:

- Improper Key Management
- Distribution of private keys
- Distribution of system wide public parameters
- Replay attacks
- Lack of Virus Detection mechanism

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

A. Key Generation using Elliptic Curve Cryptography

The proposed system eliminates those vulnerabilities by the mechanism described below:Need of proper Key management has been resolved using Elliptic Curve Cryptography. Elliptic Curve Cryptography (ECC) systems as applied to cryptography were first proposed in 1985 independently by Neal Koblitz and Victor Miller.An elliptic curve is defined with:A finite field, usually consisting in integers modulo some prime *p* (there are also other fields which can be used).A curve equation, usually y2=x3+ax+b, where a and b are constant values from the finite field.

The curve is the set of pairs of values (x, y) which match the equation, along with a conventional extra element called "the point at infinity". Since elliptic curves initially come from a graphical representations (when the field consists in the real numbers R), the curve elements are called "*points*" and the two values x and y are their "coordinates".

Suppose Alice wants to send to Bob an encrypted message. Alice and Bob creates public/private keys by agreeing on a base point, F. For that, Alice selects a secret "a" and computes Public Key, PA = a * F. Similarly, Bob selects his own secret called "b" and his Public Key, PB = b * F. They then exchanges their public keys to each other in order to create their corresponding private keys. When Alice gets the public key of Bob, she computes her private key, PrA = a * PB. Similarly, Bob computes private key, PrB = b * PA when he gets Alice"s public key.Now, each nodes will generate their own public, private key pairs.

B. Bundle:

The DTN Bundle Security Protocol (DTNBSP) defines the format andformat and processing of the blocks used to implement the Bundle Protocol (Bundle), which is then simplified for this proposed system.The bundle (packet) consists of Primary Block and Payload Security Block (PSB) which is depicted in the Figure 2 and 3.

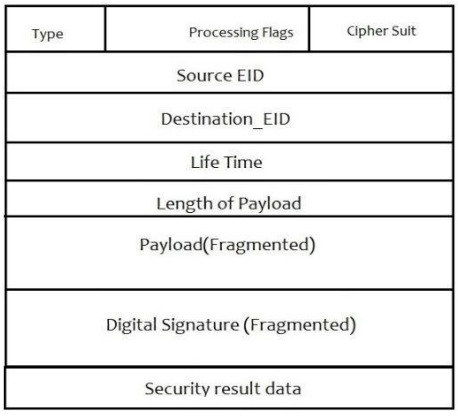

Figure 2:Bundle Format

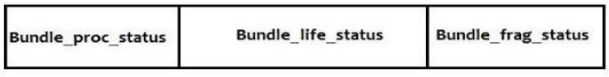

Figure 3: Processing flags

Fields from "Type" to "Length of Payload" is known as "Primary Block" and the rest is known as "Payload Security Block"(PSB).Below is the detailed description about each field in a Bundle.

C. File Sending (At the sender side)

Suppose Client A and B joined in a Delay Tolerant Network. Now, Client A requests for a connection with the Client B if he wishes to send a file to B, Client B in response, checks for its availability and then accepts the request. In the meantime, both the clients agrees up on a public key and generates their own private keys using Elliptic Curve Cryptography (ECC) algorithm (as described earlier).

Now, the public key of Client A is available with Client B and vice versa. Client A then picks the file that he wishes to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

send. He then packs the file inside a Bundle using the Bundle Security Protocol (described earlier).The in depth explanation how data is packed inside a bundle will be explained in the next section. After selecting the file to be transferred, Client A starts forming the primary block and Payload Security Block of the bundle. Primary Block is explained below.

1. Type: Explains the type of protocol used to transfer a file in DTN. Normally, it will be a string value called "Bundle Security Protocol" and is added against this field.
2. Processing Flags: The field which decides whether the Bundle to be processed or not. It has 3 sub flags. They are:

   a. Bundle_frag_status: If the file is in a fragmented (divided into more than 2 parts) structure,this filed is set to 1,else set to 0.
   b. Bundle_life_status: initially it is set to 0.It changes only when it reaches the destination.
   c. Bundle_proc_status: initially it is set to 0.It changes only when it reaches the destination.

3. Source End Point ID (Source_EID): This field contains IPv4 (32bits) IP address of the source machine (here Client A"s ip address).
4. Destination End Point ID (Dest_EID): This field contains IPv4 (32 bits) IP address of the destination machine (here Client B"s ip address).
5. Life Time: Client A adds the system"s time in which the Bundle has been formed and some seconds needed for the file transfer and store them as byte.
6. Length of Payload: Length of the file content (Payload) in bytes.
7. Cipher Suit: contains name of algorithms used for encryption/decryption and hashing. Next, fields comes under Payload Security Block is explained below.
8. Payload (Fragmented): gets the content of the file and the divides it into different parts and stores in this field. The payload formation is depicted in the Figure 4

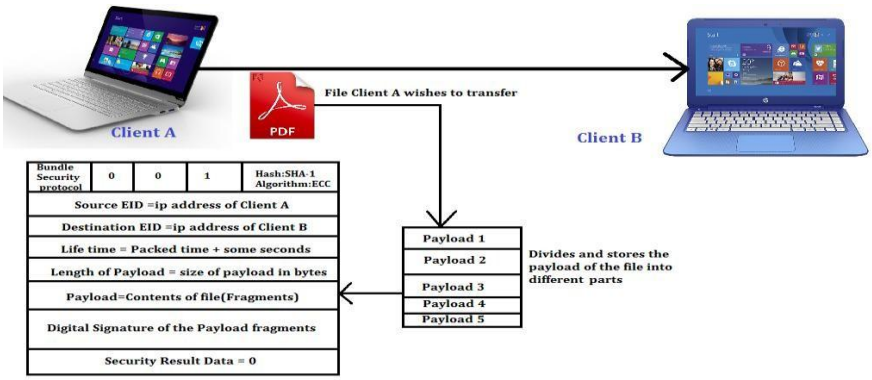

Figure 4: Bundle-Payload Formation

9. Digital Signature of payload (fragmented): Here top-and-Tail Virus Scanning method is used. Get a copy of the "Payload" field. Each fragment is the taken one by one and take the top - tail parts of it. Using any hashing algorithms such as SHA or MD5, get the hashed content of it which is now known as its Digest.

   Now, encrypt the Digest using the private key of Client A generated using ECC algorithm in order to get the Digital Signature of it. Do it for every other fragments and then store each Digital Signatures in this field. The Digital Signature of payload formation is depicted in the figure 5.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

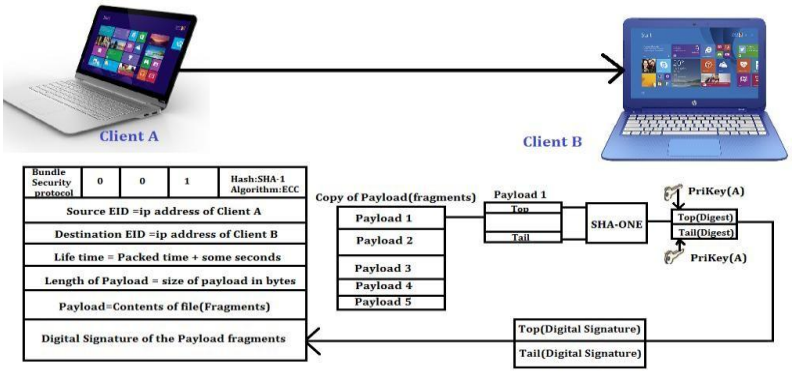

Figure 5: Bundle-Digital Signature of payload formation

10. Security Result Data: Initially (at the sender side) it always sets to 0. Bundle is now encrypted using the public key of the receiver and then sends it to the destination machine (here it is Client B).

At last, the Bundle get encrypted using the Public Key of Client B which is shown in the Figure 6.

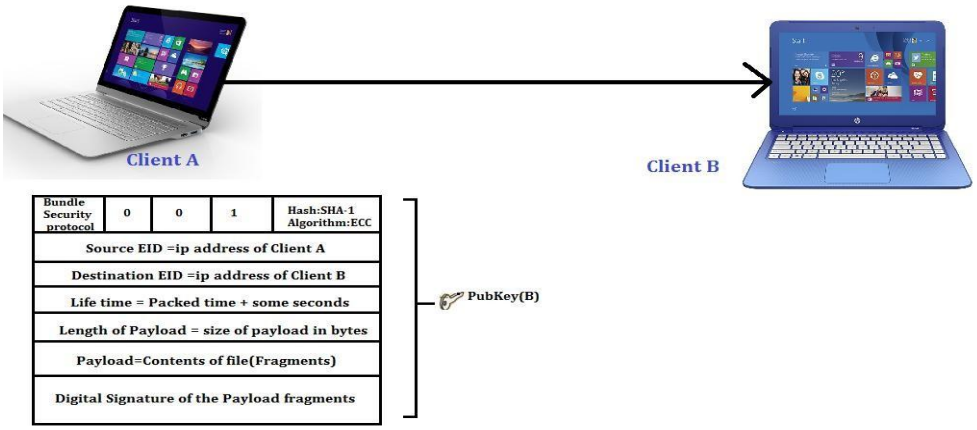

Figure 6: Encrypting the bundle

D. File Receiving

Upon receiving the bundle from the source (Client A), recipient machine (client B) decrypts the Bundle using its own Private Key. It then extracts and check each field in the bundle. Now, it checks "Type" field whether it contains the string "Bundle Security Protocol" or not. If true, it go for "Bundle_frag_status" in the "Processing Flag" field. If that field contains "1", it left the other sub flags and suddenly migrates to Source_EID field as well as Destination_EID and checks for the validity of them and sets the sub flag "Bundle_proc_status" of the "Processing Flag" field to 1.Else to 0.

It then moves on the next field called the "lifetime". Receiver compares the current time of the recipient machine

against the value inside the "lifetime" field. If the current time exceeds the lifetime, then set the sub flag field "Bundle_ life_status" of "Processing Flag" to 0 and request the sender to resend the packet. Else, set it to 1.Then now

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

proceed to extract the value of next fields called, "Length of Payload", „Payload" (Fragmented).Now, get the length of the "payload
(fragmented)" in the destination machine. Compare it against the "length of payload" field. If they are not equal, then set
"Bundle_proc_status" to 0, and request the sender to resend the packet. Else, go for the Top-and-Tail Virus scanning technique.
Recipient now extracts the, "Digital Signature of Payload" (fragmented) [DSP] field and takes the "Payload" field too. From the DSP, recipient takes each digital signature, extract the Digests using the public key of the receiver. Now, take the corresponding top-tail fragmented parts of the field "Payload" and do hashing on the Payload top-tail fragments in order to get the Digests using the specified hashing algorithm in the field "Cipher Suit".

Compare the value of Digests from the "Payload" as well as from the "Digital Signature". If they are equal then set
Security Result Data field to 1, else to 0.Do it for every fragments. At the end, extract the security Result data value. If it is 1, Bundle_proc_status sets to "1" and then the packet get accepted. Else, set to 0, and then discard the Bundle. Therefore we can claim for Confidentiality, Integrity and Availability through this method. This process is shown in the Figure 7.

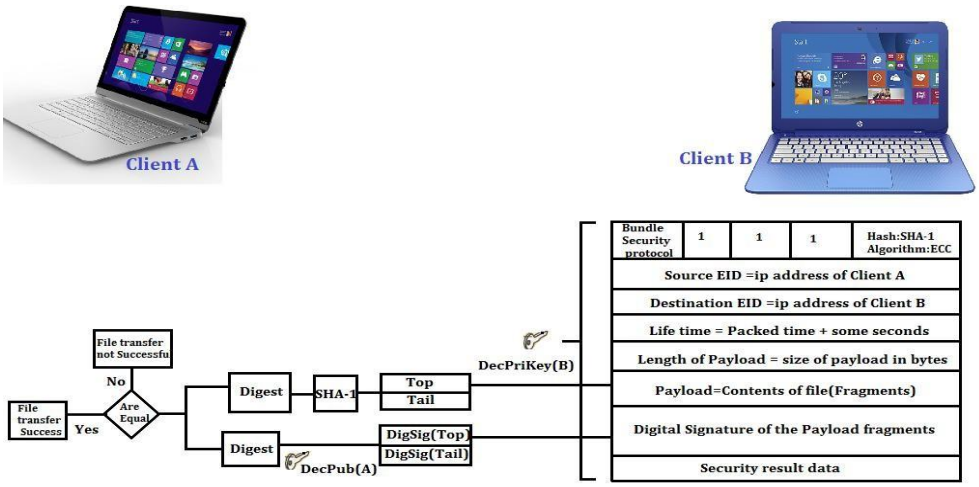

Figure 7: Decryption and Verification of Bundle

IV. EXPERIMENTAL RESULTS

The new scheme called "Effective Transmission of Bundle in Delay Tolerant Networks" has been designed. It can effectively detect virus injection in a file and therefore assure confidentiality, integrity and availability using Bundle Security Protocol. Conducted an experiment: with the self-developed tool called SDTN (Secured Delay Tolerant Network).We have installed and tested the SDTN program in Acer PC and HP.SDTN has been written and developed in Java 7.0 using NetBeans IDE 7.0.1.

In order to test the capability of detecting virus, we have installed SDTN tool in those machines which are having JVM (Java Virtual Machine) capability. We have installed SDTN in a machine with ip address 192.168.43.94.The Figure 8 shows the other active clients in a Delay Tolerant Network with their IP address.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

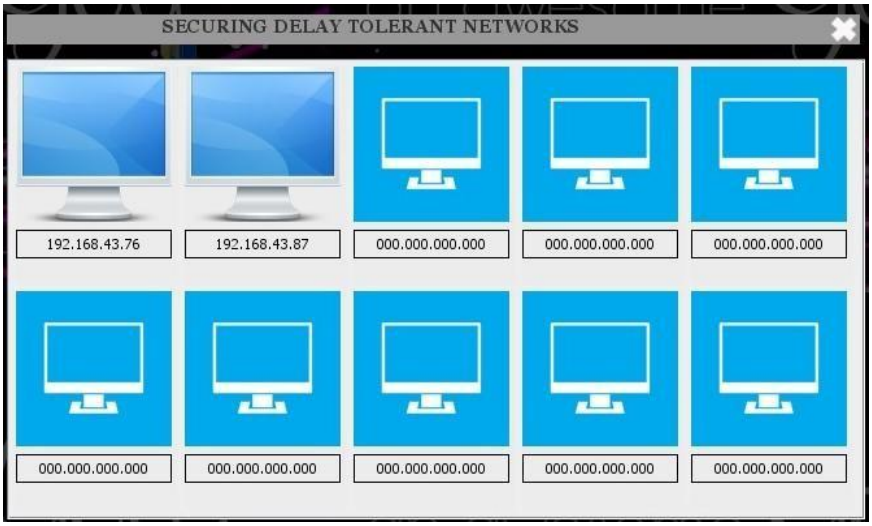

Figure 8: Active Clients in SDTN

If sender with ip 192.168.43.94 want to send a file to the client with ip address 192.168.43.87, just click on it. A sub frame called "options" will be displayed with three buttons called, Browse File, Send File, Inbox is shown in the Figure

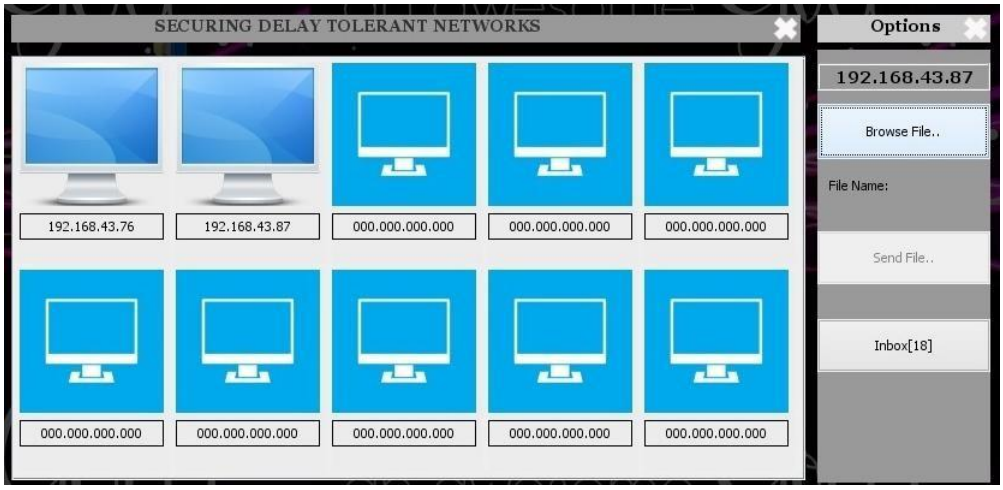

Figure 9: Sub Frame for sending a file.

Send File button will be deactivated until it selects a file. Now, it can select a file that it wishes to send using the button Browse File is shown in the Figure 10.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

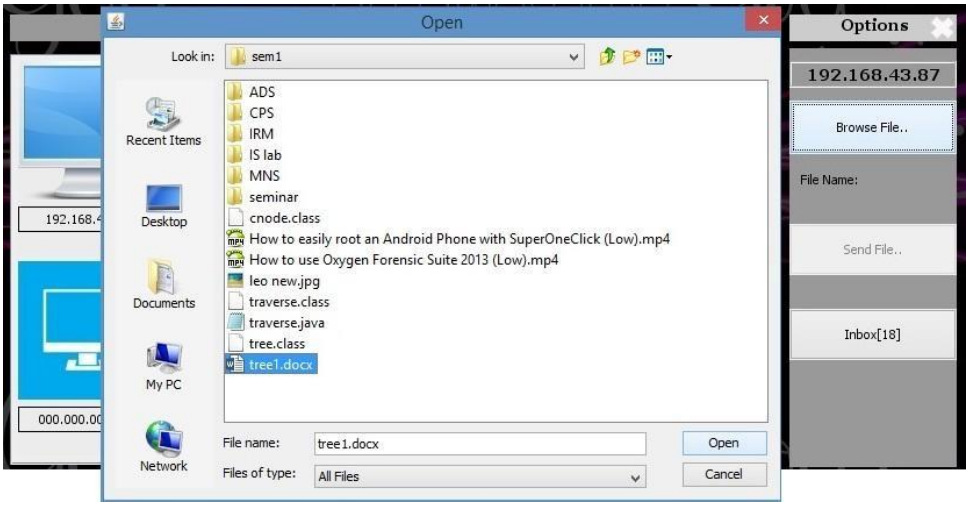

Figure 10: File browsing

After the selection, press the button Send File. At this time as explained in the proposed system, Bundle will be formed and transfers the file to the destination machine.

If the file has been reached securely, a message "File has been successfully reached" will be displayed at the destination machine. Otherwise, the message "File has been corrupted" will be displayed and automatically tells the sender to resend the Bundle. Inbox panel will be automatically displayed at the destination machine which shows the list of received files as shown in the Figure 11.

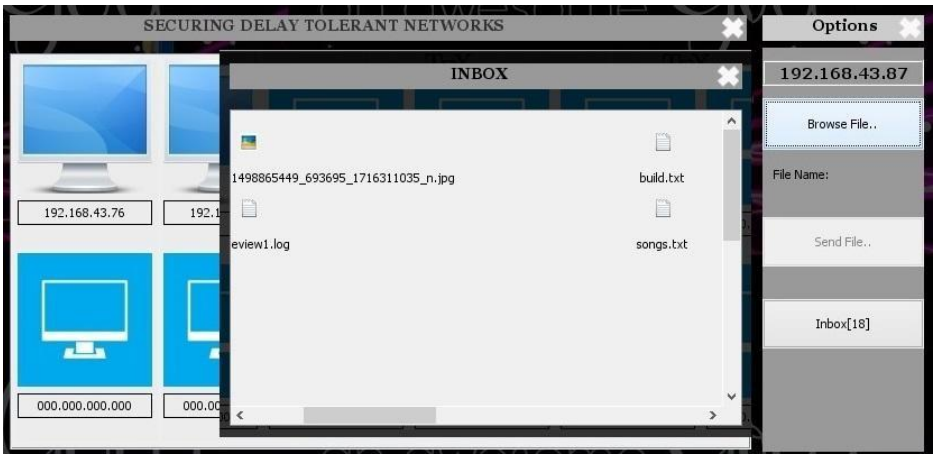

Figure 11: Inbox Panel

The tool for detecting virus and well as providing secure data transfer called the SDTN has been also successfully tested on Acer and HP and find it as efficient for detecting, preventing viruses and secure data transfers. This schemecause lesser communication overhead and sends the file without any delays and therefore assures confidentiality, integrity and availability and also it is a solution against attacks such as DoS, Man-In-The-Middle etc.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

V. CONCLUSION AND FUTURE WORK

Delay-tolerant networking (DTN) is an approach to computer network that solves the technical issues in heterogeneous network that face the unpredictable loss of continuous network connectivity, long delay, high error rates. The new application called Secured Delay Tolerant Networks (SDTN) has been designed for securing Delay Tolerant Networks. It provides security for the data sent among the nodes in the DTN. Pattern matching of viruses is an effective method in detecting viruses. Both the pattern matching method for detecting viruses and using Bundle Security Protocol gives more strengthen DTN. This scheme is designed in such a way that it causes lesser communication overhead.Application Secured Delay Tolerant Networks, is not able to detect the viruses which are obfuscated. As a part of my future work, I would like to incorporate the method to find the obfuscated viruses as well as to design more strengthen

REFERENCES

1. EvgeniosKonstantinou Supervisor: Dr. Stephen WolthusenMetamorphic Virus: Analysis and Detection Department of Mathematics Royal
Holloway, University of London Egham, Surrey TW20 0EX, England http://www.rhul.ac.uk/mathematics/techreports
2. S. Symington, S. Farrell, H. Weiss, “Bundle Security Protocol Specification” Trinity College Dublin Category: Experimental, ISSN:
2070-1721
3. Pirzada, Sohail Abbas, MadjidMerabti, and David Llewellyn-Jones, "Reputation System in MANETs", http://www.cms.livjm.ac.uk/pgnet2010/makecd/papers/2010046.pdf.
4. Kejun Liu and Jing Deng, "Reputation values constructed using the ACK messages sent by the destination node", http://dl.acm.org/citation.cfm?id=986876..
5. K. Aberer and Z. Despotovic, "work on the use of reputation systems for P2P networks",http://dl.acm.org/citation.cfm?id=776346.
D.Shama and A.kush,"GPS Enabled E Energy Efficient Routing for Manet", International Journal of Computer Networks (IJCN), Vol.3,
Issue 3, pp. 159-166, 2011.
6. Vellambi and F. Fekri, "challenges of providing secure communication in DTNs", in proc., International Journal of Advanced
Computational Engineering and Networking 2012.
7. J. Su, K. Chan, A. Miklas, K. Po, A. Akhavan, S. Saroiu, E. de Lara, and A. Goel, “A preliminary investigation of worm infections in a
bluetooth environment,” in Proc.ACM WORM, 2006.
8. Naveed Ahmad, Haitham Cruickshank, Zhili Sun, “ID Based Cryptography and Anonymity in Delay/Disruption Tolerant Networks”, Centre for Communication Systems Research, University of Surrey Guildford, Surrey, UK
9. Leona Antony, Asst.prof.Harlay Maria Mathew, Prof.P.Jayakumar: "A New Steganographic Approach Using Sudoku with Digital
Signature", International Journal of Computer Engineering and Technology (IJCET) Volume 5,Issue 12,2014,ISSN 0976-
6367(PRINT),ISSN 0976-6375(ONLINE)
10. Y. Li, P. Hui, L. Su, D. Jin, and L. Zeng, “An optimal distributed malware defense system for mobile networks with heterogeneous devices,” in Proc. IEEE SECON, 2011.
11. Ulrich Bayer,PaoloMilaniComparetti,ClemensHlauschek,ChristopherKruegel and EnginKirda, "Scalable, Behavior-Based Malware
Clustering" in proc IEEE 2008. [12] W. Hsu, T. Spyropoulos, K. Psounis, and A. Helmy, “Modeling time-variant user mobility in
wireless mobile networks,” in Proc. IEEE INFOCOM, 2007.
12. E. Daly and M. Haahr, “Social network analysis for information flow in disconnected delay-tolerant MANETs,” IEEE TMC, vol. 8, no. 5, pp. 606–621, 2009.
13. S. Kamvar, M. Schlosser, and H. Garcia-Molina, “The eigentrust algorithm for reputation management in P2P

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 11, November 2015

networks." in Proc. ACM WWW, 2003.
14. S. Buchegger and J. Boudec, "Performance analysis of the CONFIDANT protocol," in Proc. ACM MobiHoc, 2002.
15.S. Cheng, W. Ao, P. Chen, and K. Chen, "On modeling malware propagation in generalized social networks,"IEEE Comm. Lett., vol. 15, no. 1, pp. 25–27, 2011.
16.Y. Li, P. Hui, L. Su, D. Jin, and L. Zeng, "An optimal distributed malware defense system for mobile networks with heterogeneous devices," in Proc. IEEE SECON, 2011.