PERFORMANCE ANALYSIS OF TRANSPORT LAYER BASED Hybrid Covert Channel Detection Engine

Anjan K[1], Srinath N K[1], Jibi Abraham[2]

[1] Department Of Computer Science and Engineering,
R V College of Engineering,
Bangalore,India
[2] College of Engineering, Pune, India

ABSTRACT

Computer network is unpredictable due to information warfareand is prone to various attacks. Such attacks on network compromiseson the most important attribute, the privacy. Most of such attacksare devised using special communication channel called Covert Channel".The word Covert" stands for hidden or non-transparent.Network Covert Channel is concealed communication paths within legitimatenetwork communication that clearly violates security policies laiddown. Non-transparency in covert channel is also referred to as trapdoor.A trapdoor is unintended design within legitimate communication whosemotto is leak information. Subliminal channel, a variant of covert channelworks similarly as network covert channel except that trapdoor is setin cryptographic algorithm. A composition of covert channel with subliminalchannel is the Hybrid Covert Channel". Hybrid covert channelis the homogeneous or heterogeneous mixture of two or more variantsof covert channel either active at same instance or at different instanceof time. Detecting such malicious channel activity plays a vital role inremoving threat to legitimate network.In this paper, we introduce new detection engine for hybrid covert channelin transport layer visualized in TCP and SSL. A setup made onexperimental test bed (DE-HCC9) in RD Lab of our department. Thepurpose of this study is to introduce few performance metrics to evaluatedetection engine and also to understand the multi-trapdoor natureof covert channel.

KEYWORDS

Covert Channel, Subliminal Channel, Hybrid Covert Channel,Network Security, Trapdoors

1. INTRODUCTION

Recent tremendous growth in network has increased more awareness about security aspects amongst spectrum of technical fraternity. It's unfortunate that there are too few people working on securing channel against threat of covert channel. Detection methods are still at its infancy and depend on the structure of network under consideration.

Covert Channel[1,2,3] is a malicious conversation within a legitimate network communication. Covert Channels clearly violate the security policies laid down by the network environment allowing the information leak to the unauthorized or unknown receiver. Covert Channels do not have concrete definition and are scenario oriented. Covertness in these channels exhibit behaviors like multi-trapdoor and protocol hopped where in which channeling is not constrained to pair of communication entities. A fundamental covert channel can be visualized in the figure.1 depicting the covert communication model employed in the covert channel with pre-shared information encoding and decoding scheme between the covert users.

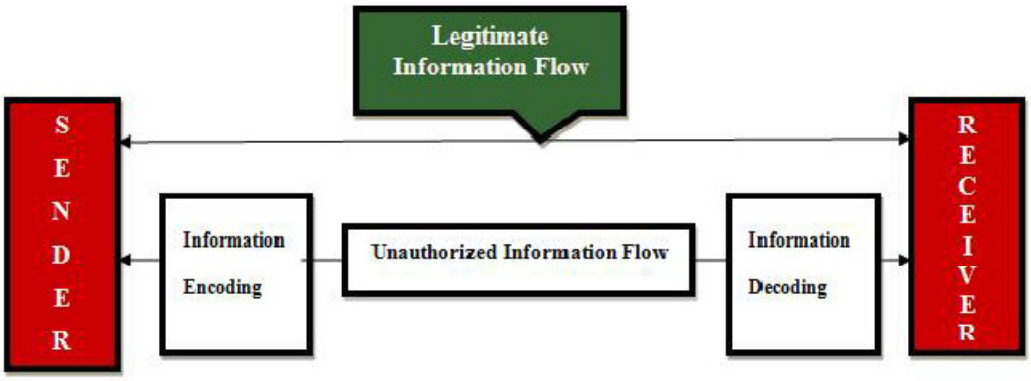

Figure 1:Covert Channel Visualization

Covert channel can also exist between threads in process or processes in operating system or amongst distributed entities. The focus here is on the design exploration in the specific network protocol and in security protocol. Covert channel is associated with similar terminologies like **side channel** or **stegnographic channel** or **supraliminal channel**, these literature terms are indifferent to each other and stand on the motto of promoting covertness in different forms or scenarios in a communication model over legitimate network.

Covert Channels in general exhibit some characteristics: **Bandwidth and Covertness Index**. The bandwidth is the amount of covert data sent in the network as per the figure 1. This can be formulated using the Shannon's Channel Capacity –

$$C_{covert} = log_2\left(1 + \frac{T}{N}\right)$$

Where T is the flow of Covert data and N is the Noise in the channel during transmission. For the network channel with covert communication the total bandwidth of the channel C always will be

$$C_{covert} < C$$

The Covertness index [16] is the strength of the detection of the trapdoor placed in the network protocols which determines the appropriate detection methods to be employed. The covert channels are broad classification is described in [5].

Hybrid Covert Channel(HCC) [5], a variant of covert channel is defined as homogeneous or heterogeneous composition of two or more covert channel variants existing either at same instance or at different instance of time. Hybrid Covert Channel may be composed of many covert channels and does not have fixed composition. Due to this it is impossible to detect all the possible channels in HCC at real time. HCC can also behave as single coherent channel with characteristics as multi-trapdoor and protocol hopped [10]. Hybrid Covert Channel here as shown in figure 2 is visualized as a combination of simple network covert channel in TCP and subliminal channel in SSL, both being transport layer protocols.

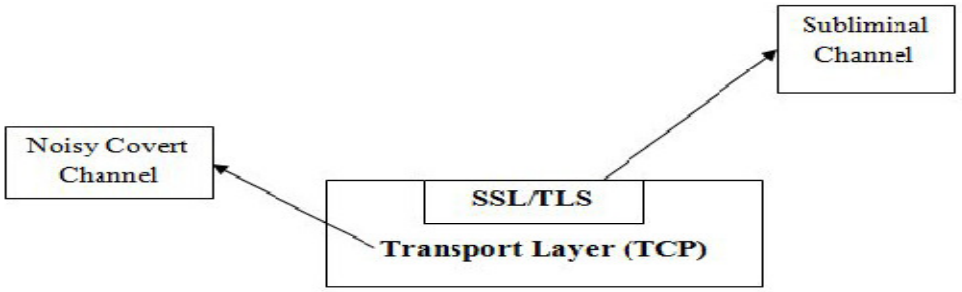

Figure 2: Hybrid Covert Channel in Transport Layer

Further section of this paper covers various detection methods and system totackle the hybrid covert channel based on the proper detection method. Section2 explores related work. Section 4 gives brief insight about various detectionmethodology and chosen detection method for hybrid covert channel scenario.Section 5 delineates about the system design and implementation. Section 6gives testing of the system in DE-HCC9. Conclusion and future enhancementsis provided in section 7.

2. RELATED WORK

Extensive work has been done to devise better detection methods to detect only covert channel either on live wire or on a dataset. In [7] is based on detecting covert shells by monitoring the unusual traffic in the network stream. Covert timing channels are design and detecting in [8] based on packet inter-arrival and modelling whole process as Poisson's distribution. Illegal information flows in covert channels are tracked by tracing the Message Sequence Charts (MSC) in [9]. This paper employs a statistical protocol based detection [11] to detect hybrid covert channel based on analysis made on packet headers.

3. DETECTION METHODS

Detection methods [11] are based on the anomaly or signature match in the protocols of the network stack. However, there is new covert language encoding schemes in the protocols that make sit sophisticated to detect it. The channel detection scheme must follow various rounds of checks before the alert is flashed to the administrator of the network and must actively scan the flow of information in the channel. If the same process is carried in after an attack event then the procedure is purely under Network Forensics. If the detection schemes are capable identifying a victimized resource then the process is termed as **Covert Channel Identification**. There are different methods used to detect a covert channel and it presented below –

3.1. Signature Based Detection

Signature-based is also termed as misuse based detection and is carried out actively on the network streams by searching specific patterns or signature of standard protocol. In such cases the algorithm alarms the network of a breach. The popular tool which can detect is NetCat - which is a reverse-shell communication between the internal network and a public network.

3.2. Protocol Based Detection

Protocol based detection scheme is simple profiling of each protocol used in communication. This is refereed to a ***deep packet analysis*** where the each header is scanned to understand its standard values. The standard profile of a protocol is the protocol specification described in their RFC's. Covert_TCPtool manipulates sequence number field, ACK Field in TCP and IP ID in IPv4 packet for the covert communication.

3.3. Behavioral Based Detection

Behavioural based detection scheme is sophisticated scheme as it monitors user profiles, resource profiles and reference profiles. It detects the unusual behaviour in the network and is performed in real-time. The detection is based on deviation of usage of the network from normal scenarios. A simple instance can be multiple packet transmission from a source with same sequence number and keeping the traffic of the network it is peak.

3.4. Other Approaches

Other Approaches includes detection based on the supervised learning schemes like neural network. Neural network approach involves training the network for `T' period until required accurate values to trigger the alarm process by the detection engine. Scenario based Bayes interference is to set up a system in which each suspicious matched signature (hypothetical attack) found in the monitored data stream is part of a global set (symptoms) and use each global set to calculate, with a Bayes inference, the probability for a known attack to be on hold knowing the P(Hypothetical attack / Symptoms) probability.If the detection engine finds a suspicious scenario which probability value is greater than a set threshold, an alarm process is triggered by the detection engine.

Above categorization can also behave as either statistical or probabilistic. A statistical approach is to run the detection engine for `t' hours and record an amount of data `D'. This period is called as learning period and such approach helps to increase the accuracy and also to set the threshold value for the alarm process. A probabilistic approach is to set a probability for the specific event S that occurs after P, Q and R as Y\%. This helps the detection engine to tune itself to such event in its running period.

4. SYSTEM DESIGN AND IMPLEMENTATION

Major Design Criteria

HCC in transport layer is combination of trapdoors placed in TCP and backdoors placed in TLS. The design of the channels with respect to TCP and TLS are different. It works on simple packet capture utility and then analysis of payload and headers. TCP payload will content – TLS/SSL content and process forming the content is specified in the figure 3.

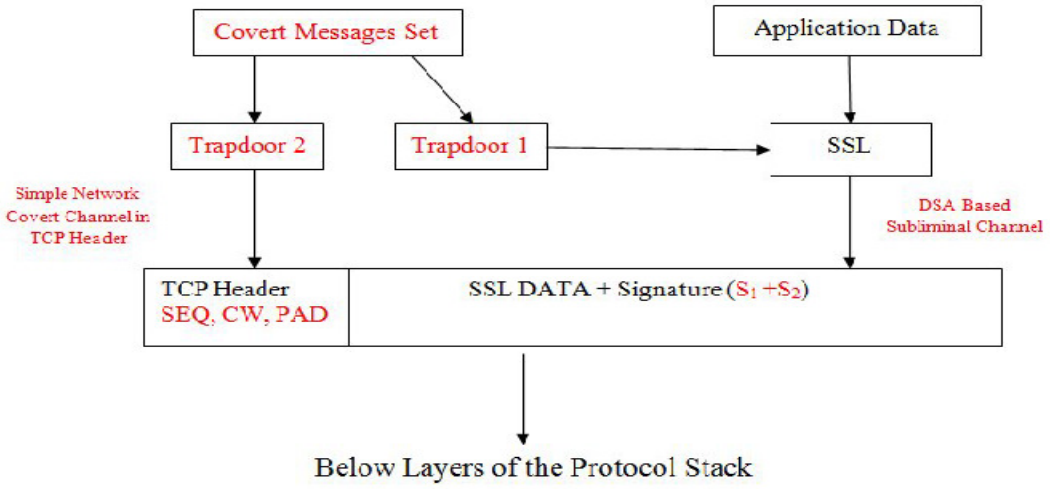

Figure 3:Hybrid Covert Channel Formation

In figure 3, words marked with red refer to covert process and those with black refer to legitimate process. Channel has to constructed to test the detection engines accuracy and its covertness index. This would suggest the best suited detection schemes to be used for achieve positive detections. The approach here can be combination of Protocol and Signature based schemes also referred to as **Statistical Protocol Based Detection**.

Designing Hybrid Covert Channel takes two different routes discussed in the coming sub-sections. With reference to figure 3, flow of design follows first subliminal channel in SSL and then the simple network covert channel in TCP.

4.1Designing Subliminal Channel in TLS/ SSL

SSL had wide range of cipher algorithm that assist in secured communication. One such algorithm is the DSA that provide authentication service. Subliminal Channel is created in DSA as per [13]. Practically this can done in following ways -

1. Covert user generates a random number and provides it during the signature generation process.
2. Covert user replaces system generated public-private keys with the keys that covert process has generated. This may even content bit and bytes of the covert message to be communicated.
3. The Signature component used in the TLS will content the subliminal message generated in 2. This will be sued as communication medium for the reciver to understand the message sent by the covert sender.
4. Programmatically this can be accomplished either with OpenSSL or JSSE secure sockets.

4.2Designing Simple Network Covert Channel in TCP

The process of the covert channel generation in network protocol as described in [5] where the covert sender places his covert data in covert vulnerable fields like Sequence Number, Flags, Ack, options and reserved. The focus here is on constructing simple network covert channel, with

specific focus on Sequence number, padding and Flags fields of the TCP. Direct access of the network card is required to send this TCP packet by the covert user. This can accomplished in following ways –

1. Jpcap libraries in Java that gives direct control of the interface to developer, here a covert user.
2. BSD socket in Linux where socket creation can be done in the raw mode of operation to create custom packet and informing the kernel not append checksum as this done the developer.

4.3 Design and Implementation of Detection Engine

The design of the detection engine takes two stages- one for detecting the subliminal channel in TLS/SSL and the other is for the simple network covert channel in TCP. In TCP based covert channel, TCP packet must be available for diagnosis; this can be accomplished by employing a protocol sniffer. In TLS/ SSL payload, it assumed that covert user has replaced the original supplied keys and also random number is manipulated. In such cases randomness test for both keys and the random number will prove that fact of trapdoor placed by covert party.

Detection Engine Algorithm:

```
Step 1: Capture TCP packets from Network Interface using protocol
sniffer fromuser specified network device
Step 2: Store the TCP packet in database by parsing each fields.
Step 3: Analyse the TCP header for the covert vulnerable fields.
Step 4: Analyse the signature component in the TLS which is a
payload in TCP payload and testifythe key against Randomness
tester
Step 5: Log the entries of the covert and subliminal activity.
Step 6: Compute the performance graph and detection
contentcomputation from the each session data set.
```

5. TESTING

Testing results are based on the design consideration made in [6]. DE-HCC9 test bed performance will be based on its detection rate and detection content under different circumstances. The variables to be considered for the performance analysis are listed as follows for `n' nodes in the experimental test bed with `s' sample count and for the session `t'. Let

- αbe the total number of packet captured.
- β be the number of TCP packets captured
- γ cardinality of dataset previously collected
- T be the total number of detection made
- **t**be total number of available TCP packets in database.

- Φ Relative Detection Content with respect to β.
- η Absolute Detection Content with respect to α

Total number of TCP in database or dataset is

$$t = \gamma + \beta \qquad (1)$$

In the equation 1 if $\gamma = 0$ and $t = \beta$

The calculations for detection content are performed using the expressions.

$$\phi = \frac{T}{\beta}$$

$$\eta = \frac{T}{t}$$

The threshold value for γ is 10000 packets.

$$Average\ Detection\ rate\ \theta = \frac{\phi + \eta}{2}$$

Experiments made on DE-HCC9 indicate that packet capturing from thenetwork interface has uniform increase with respect to time. This is visualizedin graph obtained from the test bed show in figure 4.

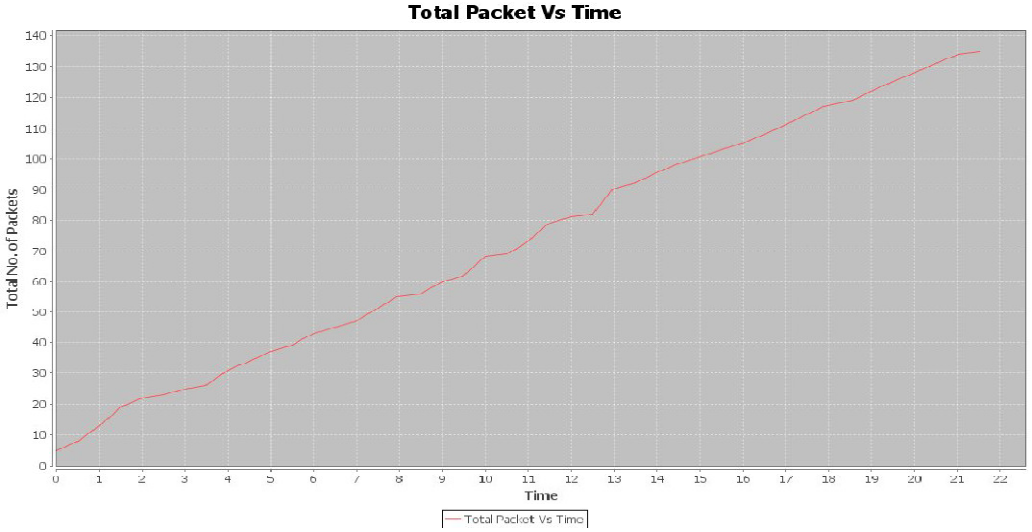

Figure 4: Total No. of Packets (α) Vs Time

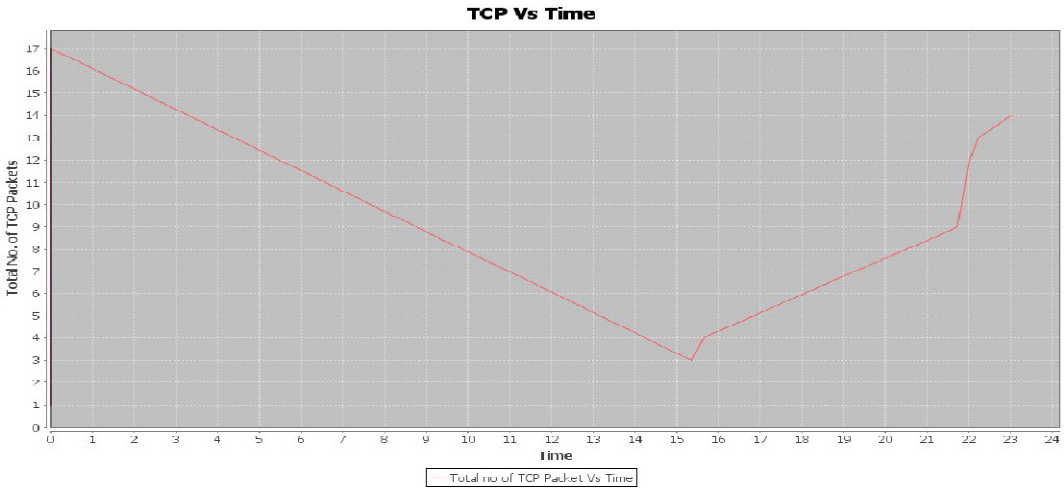

Figure 5: TCP PacktsVs Time

This figure 5 completely depends on the traffic in the subnet and node count.The detection content in TCP for 5 nodes varies between 15% - 30% and average detection rate at 70% - 97% as depicts in the figure 6. Also that detection content depends on number of times covert channel is invoked in that session. If sampling is done for infinity then these percentages decrease to small number or even negligible, which is true in the real network scenario.

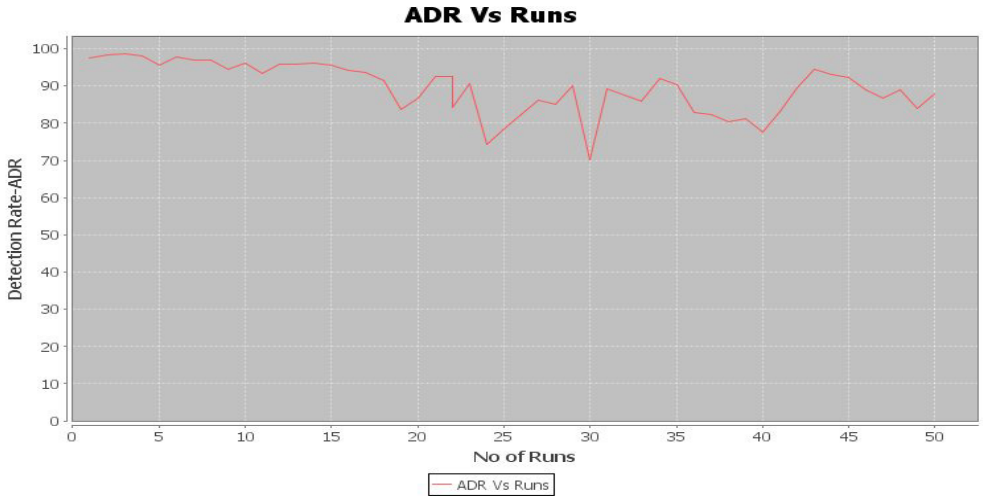

Figure 6: Average Detection Rate Vs No. of Runs

5. CONCLUSION AND FUTURE WORK

Hard Compromise on confidential information and is clearly unacceptable in presence of security measures for legitimate network. Conspiracy between communication parties is not legitimate (Covert Parties) and existence of Hybrid Covert Channel is the strongest threat in communication which should be decommissioned. Conclusion is to build system to detect the activity of Hybrid covert channel in a small scale LAN. This paper has focused such system and also introduces performance metrics to evaluate such system in experimental test bed (DE-HCC9).

The project develop is primitive attempt to detect the hybrid covet channel and further improvements include the adding following features

- To cover most of the possible covert fields in TCP packet header like acknowledgment bounce and options.
- Include elimination protocol especially suited for the scenario considered in this project called ``Spoofed Pump'' protocol.
- Further to include possible hybrid combination of covert in the TCP/IP protocol stack.
- Analyse the similar possibility of hybrid channelling in case of Ad hoc wireless network since existing of covert channel in routing algorithm headers is possible.

ACKNOWLEDGEMENT

Anjan K would like to thank Late Dr. V.K Ananthashayana, Erstwhile Head, Department of Computer Science and Engineering, M.S.Ramaiah Institute of Technology, Bangalore, for igniting the passion for research.

REFERENCES

[1] Vishal Bharti, Practical Development and Deployment of Covert Communication in IPv4, Journal on Theoretical and Applied Information Technology, Apr 2007.

[2] Sebastian Zander et.al.: Covert Channels and Counter Measures in Computer Network Protocols, IEEE communication Magazine on survey an tutorials, December 2007.

[3] SweetyChauhan, Analysis and Detection of Network Covert channel, Technical Report by Department of computer science and Electrical Engineering,University of Maryland Baltimore County, Dec 2005.

[4] EnpingLi , Scott Craver, A supraliminal channel in a wireless phone application, Proceedings of the 11th ACM workshop on Multimedia and security, September 07-08, 2009, Princeton, New Jersey, USA.

[5] KoundinyaAnjan and Jibi Abraham, Behaviour Analysis of Transport Layer based Hybrid Covert Channel, Third International Conference on Network Security and Application, Springer-Verlag LNCS series, Chennai, India, Jul 2010.

[6] Anjan K Koundinya and Jibi Abraham, Design of Transport Layer Based Hybrid Covert Channel Detection Engine, International Journal of Ad hoc, Sensor and Ubiquitous Computing, Dec 2010.

[7] SarderCabuk,CarlaBrodley,ClaySheilds, IP Covert Channel Detection, ACM Transaction on Information and System Security, Vol 12, Article 22, Apr 2009.

[8] SarderCabuk,CarlaBrodley,ClaySheilds, IP Covert Timing Channels : Design and Detection, CCS' 04, Oct 2004.

[9] Lo`icH'elouet., Claude Jard, Marc Zeitoun, Covert channels detection in protocols using scenarios, SPV'03, April 2003.

[10] Steffen Wendzel, Protocol Channels, HAKIN9,Jun 2009.

[11] Description of Detection Approaches at url –http://gray-world.net/projects/papers/html/cctde.html

[12] Description of JPcap Libraries at url-http://netresearch.ics.uci.edu/kfujii/jpcap/doc/index.html

[13] Gustavus J Simmons, The Subliminal Channel and Digital Signatures, Springer-Verlag, 1998.

[14] Jerry Banks et.al. Discrete Event System Simulation, Third edition, Prentice Hall, Jan 2001

[15] Description of Randomness test suite - JRandTester at url-http://sourceforge.net/projects/jrandtest

[16] Anjan K, Gururaja H S et.al., Covertness Analysis of Subliminal Channelsin Legitimate Communication, ADCONS 2011, LNCS 7135, pp. 582–591, 2012

AUTHOR'S PROFILE

Anjan K has received his B.E degree from Visveswariah Technological University, Belgaum, India in 2007 And his master degree from from Department of Computer Science and Engineering, M.S. Ramaiah Institute of Technology, Bangalore, India. He has been awarded Best Performer PG 2010 for his academic excellence. His areas of research includes Network Security and Cryptography, Adhoc Networks, Mobile Computing, Agile Software Engineering. He is currently working as Assistant Professor in Dept. of Computer Science and Engineering, R V College of Engineering.

Srinath N K has his M.E degree in Systems Engineering and Operations Research from Roorkee University, in 1986 and PhD degree from AvinashLingum University, India in 2009. His areas of research interests include Operations Research, Parallel and Distributed Computing, DBMS, Microprocessor. His is working as Professor and Head, Dept of Computer Science and Engineering, R V College of Engineering.

Jibi Abraham has received her M.S degree in Software Systems from BITS, Rajasthan, India in 1999 and PhD degree from VisveswariahTechnologicalUniversity, Belgaum, India in 2008 in the area of Network Security. Her areas of research interests include Network routing algorithms, Cryptography, Network Security of Wireless Sensor Networks and Algorithms Design.She is working as Professor in Dept. of CEIT, College of Engineering Pune.