MULTIPATH ROUTING FOR INTERRUPTION FORBEARANCE IN ASSORTED MOBILE AD HOC MESH NETWORKS

R. Aarthi* & K. Ramamoorthy**
* PG Scholar, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu
** Assistant Professor, Department of Master of Computer Applications, Dhanalakshmi Srinivasan Engineering College, Perambalur, Tamilnadu

Abstract:

Wireless Ad hoc Mesh Networks are self-organized networks that typically consist of a large number of such sensing devices with severely limited processing, storage and communication capabilities. In Heterogeneous Wireless Sensor Networks we implement redundancy management of heterogeneous wireless sensor networks, utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime.

Data delivery in networks is inherently faulty and unpredictable. Failures in wireless sensor networks can occur for various reasons like sensor nodes are fragile, and they may fail due to depletion of batteries or destruction by an external event and links are failure-prone, causing network partitions and dynamic changes in network topology. Additionally, the optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a Heterogeneous Wireless Ad hoc Network. Dynamic redundancy management algorithm is used to apply the best design parameter settings at runtime in response to environment changes, to maximize the Heterogeneous Wireless Sensor Networks lifetime. Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in Wireless Sensor Networks.

Index Terms: Heterogeneous Wireless Sensor Network, Ids– Intrusion Detection System Security & Ad-Hoc Mesh Network.

1. Introduction:

Wireless Ad hoc Mesh Networks are self-organized networks that typically consist of a large number of such sensing devices with severely limited processing, storage and communication capabilities. In Heterogeneous Wireless Sensor Networks we implement redundancy management of heterogeneous wireless sensor networks, utilizing multipath routing to answer user queries in the presence of unreliable and malicious nodes. The key concept of redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. We formulate the tradeoff as an optimization problem for dynamically determining the best redundancy level to apply to multipath routing for intrusion tolerance so that the query response success probability is maximized while prolonging the useful lifetime. Data delivery in networks is inherently faulty and unpredictable. Failures in wireless sensor networks can occur for various reasons like sensor nodes are fragile, and they may fail due to depletion of batteries or destruction by an external event and links are failure-prone, causing network partitions and dynamic changes in network topology. Additionally, the optimization problem for the case in which a voting-based distributed intrusion detection algorithm is applied to detect and evict malicious nodes in a Heterogeneous Wireless Ad hoc Network. Dynamic redundancy management algorithm is used to apply the best design parameter settings at runtime in response to environment changes, to maximize the Heterogeneous Wireless Sensor Networks lifetime. Multipath routing is considered an effective mechanism forfault and intrusion tolerance to improve data delivery in Wireless Sensor Networks

The nature of mobile computing environment makes it very vulnerable to an adversary's malicious attacks. First of all, the use of wireless links renders the network susceptible to attacks ranging from passive eavesdropping to active interfering. Unlike wired networks where adversary must gain physical access to the network wires or pass through several lines of defense at firewalls and gateways, attacks on a wireless network can come from all directions and target at any node.

Damages can include leaking secret information, message contamination, and node impersonation. All these mean that a wireless ad-hoc network will not have a clear line of defense, and every node must be prepared for encounters with an adversary directly or indirectly.

The rapid proliferation of wireless networks and mobile computing applications has changed the landscape of network security. The nature of mobility creates new vulnerabilities that do not exist in a fixed wired network, and yet many of the proven security measures turn out to be ineffective. Therefore, the traditional way of protecting networks with firewalls and encryption software is no longer sufficient. We need to develop new architecture and mechanisms to protect the wireless networks and mobile computing applications.

Two major problems to be solved for the issue of intrusion forbearance through multipath routing is: how many paths to use and what paths to use. Our Redundancy management for both intrusion and fault tolerance through multipath routing and intrusion detection through voting-based Intrusion Detection System design to maximize the system lifetime of a Heterogeneous Wireless Sensor Networks in the presence of unreliable and malicious nodes.

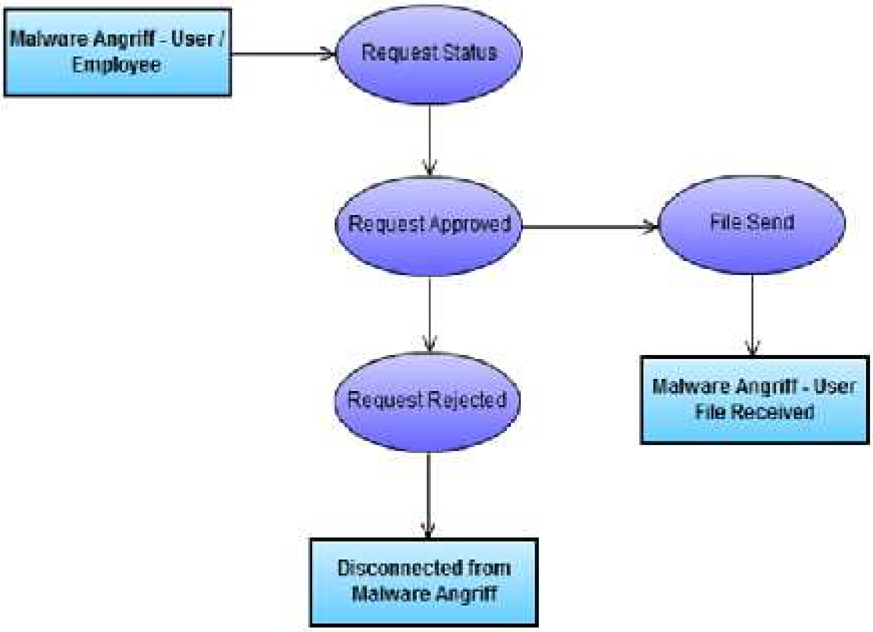

Malware Angriff - User / Employee
Request Status
Request Approved
File Send
Request Rejected
Malware Angriff - User File Received
Disconnected from Malware Angriff

Figure 1: Data Flow Diagram

2. Related Works:

After analyzing the requirements of the task to be performed, the next step is to analyze the problem and understand its context. The first activity in the phase is studying the existing system and other is to understand the requirements and domain of the new system. Both the activities are equally important, but the first activity serves as a basis of giving the functional specifications and then successful design of the proposed system. Understanding the properties and requirements of a new system is more difficult and requires creative thinking and understanding of existing running system is also difficult, improper understanding of present system can lead diversion from solution.

3. Proposed Work:

The Optimal Intrusion Detection System detection interval that can best balance intrusion accuracy vs. energy consumption due to intrusion detection activities, so as to maximize the system lifetime. Redundancy management is to exploit the tradeoff between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in Wireless Networks.

Advantages:

- ✓ Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions.
- ✓ Fault detection is to use different metrics to collect symptoms of possible faults.
- ✓ Constantly monitoring network status and triggering reactive actions if necessary.
- ✓ Enforcing redundancy in the data delivery path, hoping that at least one of the paths will survive and fulfill the task of data delivery.

Module:

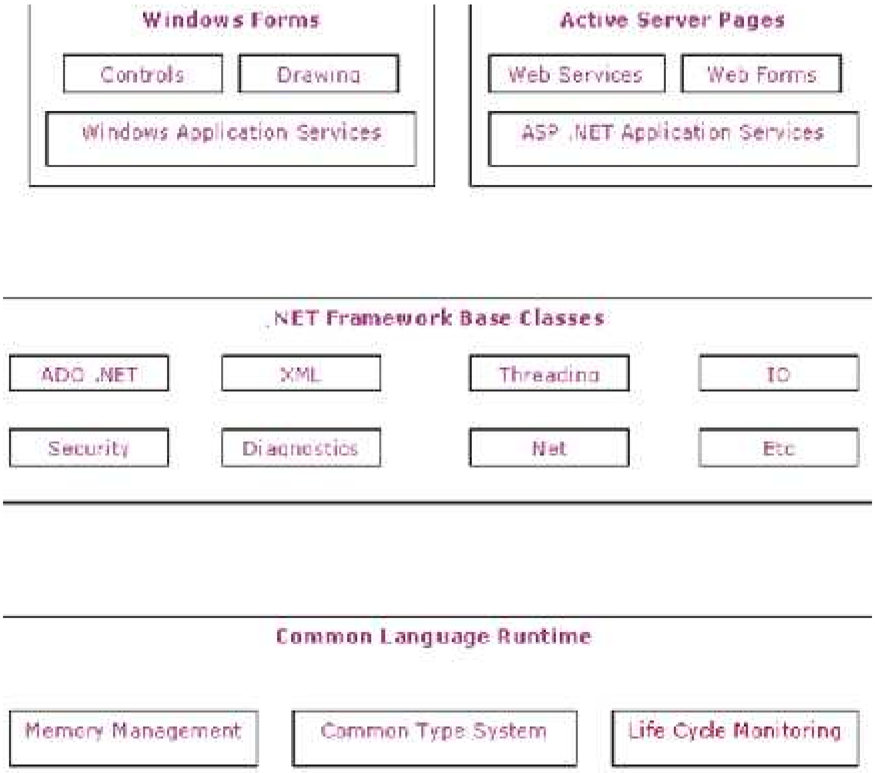
- ✓ Monitoring and analyzing traffic
- ✓ Analyzing harshness and raising anxiety
- ✓ HWSN Control Configuration
- ✓ IDS Architecture
- ✓ Dynamics of Circumstance Evolution
- ✓ Dynamic Redundancy Management

Monitoring and Analyzing Traffic: A monitor can be thought of as an instance of the ethereal network packet sniffer: It captures the traffic and displays the detailed information on it. Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. Each node in the network to produce evidences and to share them among all the nodes. Ethernet level header will consider source, destination and BSSID addresses, sequence number, frame type and subtype and the Retry flag. The agents monitor the state of the system and various kernel structures to verify the integrity of the system. Installation of appropriate security patches, by the respective users or the network operator, can immunize susceptible to the recovered states and heal infective to the recovered states. The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery. It is focused on multipath routing to improve reliability, tradeoff between QoS gain vs. energy consumption which can adversely shorten the system lifetime.

Assessing Harshness and Raising Anxiety: An infective spreads the worm to a susceptible while transmitting data or control messages to it. An affected device can also be used to attack the cellular network infrastructure by becoming part of a large scale denial of service attack. Since all nodes participate in the detection process, we extend it in order to match multiple lists. The idea is to merge one list at a time with the result of the previous merge. Most intrusion detection systems include default policies for specific operating systems. These policies vary with the design of the system being monitored. The security patches are installed at an infective node after exponentially distributed random times starting from when it is infected. Intrusion tolerance through multipath routing, are two major problems to solve: First one is how many paths to use and the second one is what paths to use.

HWSN Control Configuration: Multipath routing is considered an effective mechanism for fault and intrusion tolerance to improve data delivery in WSNs. The users were scheduled with a data size of certain size that is to be transmitted. And each user is sorted in the order of the channel quality that is the signal strength of the user.The basic idea is that the probability of at least one path reaching the sink node or base station increases as we have more paths doing data delivery. To preserve confidentiality, the HWSN executes a pair wise key establishment protocol in a secure interval after deployment.Users sub channel quality was randomly generated each frame for random set of users. In each transition a sorted best channel and round robin best channel method is used to schedule the transmit ion. The best channel attempts to maximize the data transferred per frame to measure the average data transferred per frame for both the small configuration and large configuration. The intrusion detection algorithm is applied to detect and evict malicious nodes in a HWSN.The user’s data are scheduled in the current best frame if available or the system waits for the best channel for that user to transfer the allocated frames.

IDS Architecture:



If an attack is detected, the sensor logs the attack and notifies the Director platform through the command and control interface. The Director platform displays the alarms, logs the data, and takes action on attacks detected by a sensor.IDS approach extends from considerations given to the trade-off between energy loss vs. security and reliability gain due to employment of the voting-based IDS with the goal to prolong the system lifetime. Energy efficiency is achieved by applying the optimal detection interval to perform IDS functions.With the IP blocking option, the sensor updates the access control list on the perimeter router to deny all traffic from the offending IP address. If the critical system files were modified or deleted, the alert is sent to the administrator to investigate. Systems can distribute the load associated with monitoring across available hosts on large networks, thereby cutting deployment costs.There are two approaches by which energy efficient IDS can be implemented in WSNs. One approach is especially applicable to flat WSNs is for an intermediate node to feedback maliciousness and energy status of its neighbour nodes to the sender node who can then utilize the knowledge to route packets to avoid nodes with unacceptable maliciousness or energy status. Another approach is to use local host-based IDS for energy conservation coupled with voting to cope with node collusion for implementing IDS functions.

Dynamics of Circumstance Evolution: The data come without any special requirements for auditing or logging mechanisms; in most cases collection of network data occurs with the configuration of a network interface card. We consider the case in which the transmission ranges and media scanning rate in the infective nodes is selected apriority by the worm and is fixed throughout the time interval.Redundancy management for both intrusion/fault tolerances through multipath routing and intrusion detection through voting-based IDS design to maximize the system lifetime of a HWSN in the presence of unreliable and malicious nodes.Most commercial intrusion detection products perform signature analysis against a vendor-supplied database of known attacks. The strength of signature analysis depends upon the quality, comprehensiveness, and timeliness of the attack signature housed in the IDS's search engine.For managing multipath routing for intrusion tolerance to maximize the system lifetime. They specify control actions taken by individual nodes in response to dynamically changing environments. The node population density is evolving because of some nodes being compromised and some being detected and evicted by the IDS dynamically.

Dynamics Redundancy Management: The proposed redundancy management of heterogeneous wireless sensor networks (HWSNs) used to utilizing the multipath routing to answer user queries in the presence of unreliable and malicious nodes. We solve the issues like trade-off between energy consumption vs. QoS gain in reliability, timeliness and security with the goal to maximize the lifetime of a clustered HWSN while satisfying application QoS requirements in the context of multipath routing. The key concept of our redundancy management is to exploit the trade-off between energy consumption vs. the gain in reliability, timeliness, and security to maximize the system useful lifetime. A novel probability model is used to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of nodes and the intrusion invocation interval under which the lifetime of a HWSN is maximized. The effective redundancy management of a clustered HWSN to prolong its lifetime operation in the presence of unreliable and malicious nodes. The optimal amount of redundancy through which data are routed to a remote sink in the presence of unreliable and malicious nodes, so that the query success probability is maximized while maximizing the HWSN lifetime. The objective is to dynamically identify and apply the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of nodes and the intrusion invocation interval to maximize MTTF.

4. Experimental Analysis and Results:

A software application in general is implemented after navigating the complete life cycle method of a project. Various life cycle processes such as requirement analysis, design phase, verification, testing and finally followed by the implementation phase result in a successful project management. System implementation is an important stage of theoretical design is turned into practical system. Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective. The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

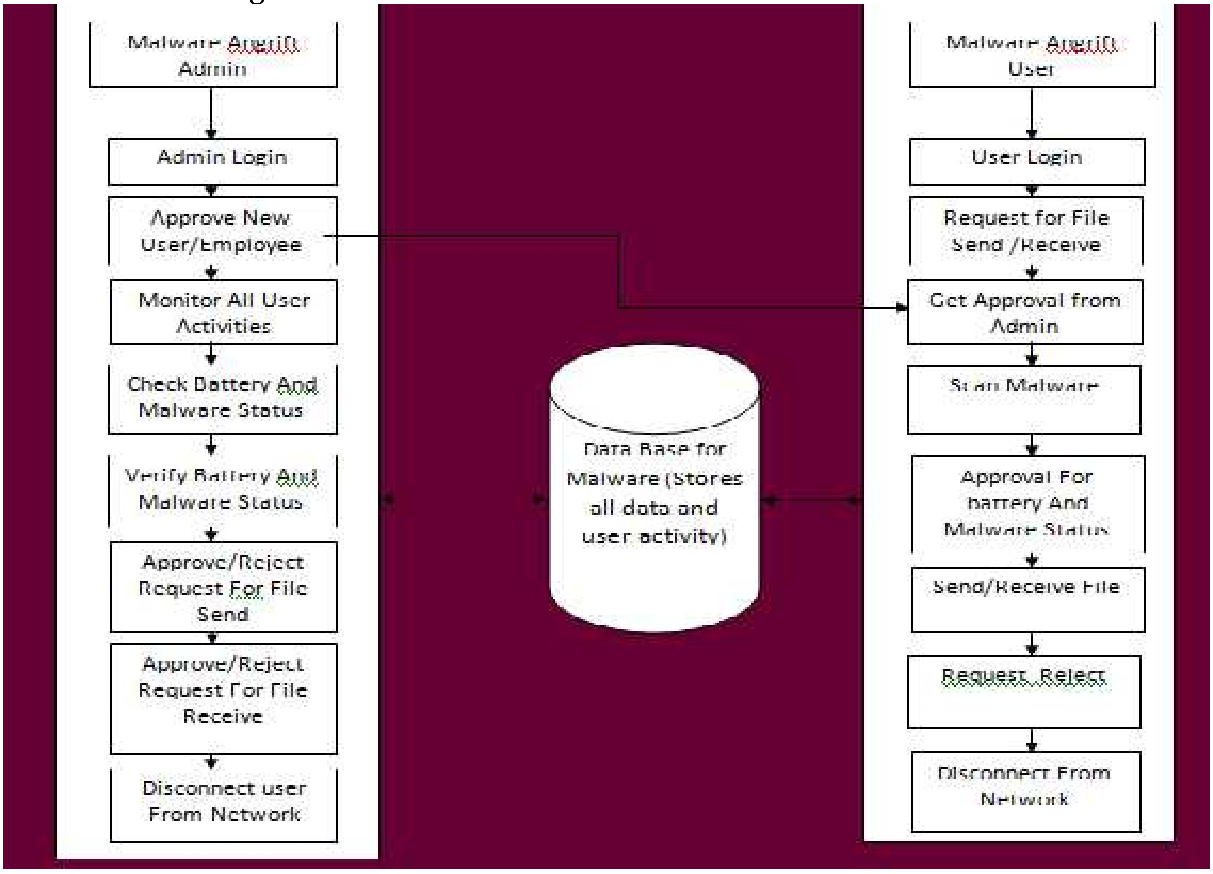
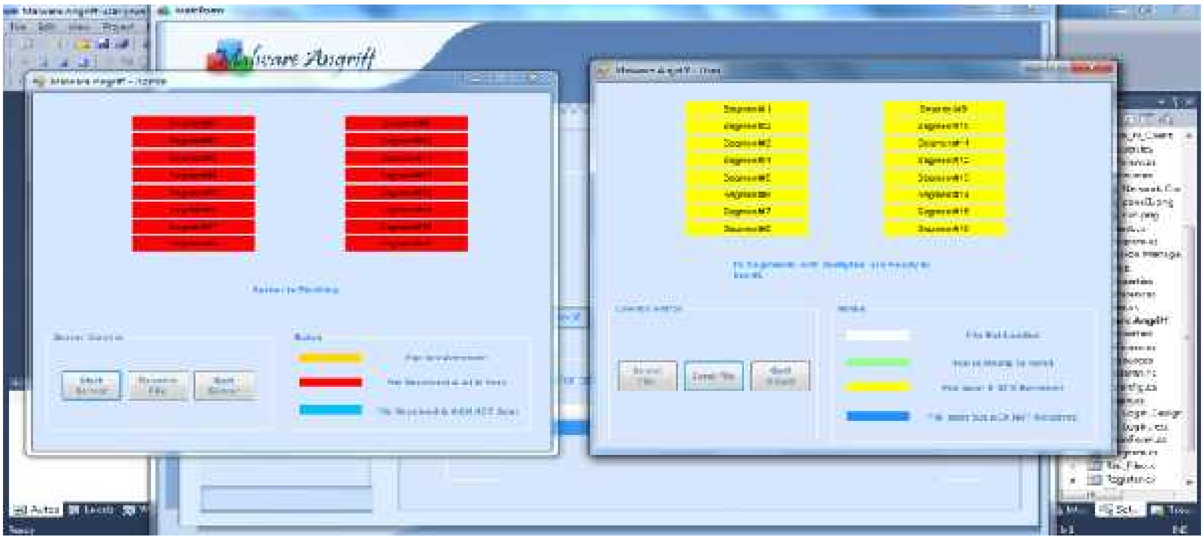

Malware Averift Admin
Admin Login
Approve New User/Employee
Monitor All User Activities
Check Battery And Malware Status
Verify Battery And Malware Status
Approve/Reject Request For File Send
Approve/Reject Request For File Receive
Disconnect user From Network
Data Base for Malware (Stores all data and user activity)
Malware Averift User
User Login
Request for File Send /Receive
Get Approval from Admin
Scan Malware
Approval For battery And Malware Status
Send/Receive File
Request Reject
Disconnect From Network

Figure 2: System Architecture

Each program is tested individually at the time of development using the data and has verified that this program linked together in the way specified in the programs specification, the computer system and its environment is tested to the satisfaction of the user. The system that has been developed is accepted and proved to be satisfactory for the user and so the system is going to be implemented very soon. A simple operating procedure is included so that the user can understand the different functions clearly and quickly. The final stage is to document the entire system which provides components and the operating procedures of the system.

Admin and User Simulation:



5. Conclusion:

In this heterogeneous application, a novel probability model is used to analyze the best redundancy level in terms of path redundancy and source redundancy, as well as the best intrusion detection settings in terms of the number of nodes and the intrusion invocation interval under which the lifetime of a heterogeneous wireless sensor network is maximized while satisfying the reliability, timeliness and security requirements of query processing applications in the presence of unreliable wireless communication and malicious nodes. And also we performed a trade-off analysis of energy consumption vs. QoS gain in reliability, timeliness, and security for redundancy management of clustered heterogeneous wireless sensor networks utilizing multipath routing to answer user queries. Finally, we applied our analysis results to the design of a dynamic redundancy management algorithm to identify and apply the best design parameter settings at runtime in response to environment changes to prolong the scheme life span.

6. Future Enhancement:

In Future, we plan to discover additional extensive malicious attacks in addition to packet dropping and bad mouthing attacks, each with different implications to energy, security and reliability, and investigate intrusion detection and multipath routing based tolerance protocols to react to these attacks. Another direction is to consider smart and insidious attackers which can perform more targeted attacks, capture certain strategic nodes with higher probability, alternate between benign and malicious behaviour and collude with other attackers to avoid intrusion detection. Lastly, we plan to investigate the use of trust or reputation management, to strengthen intrusion detection through "weighted voting" leveraging knowledge of trust/reputation of neighbour nodes, as well as to tackle the "what paths to use" problem in multipath routing decision making for intrusion tolerance in WSNs.

7. References:

1. P. Jayanthi and T. Parameswaran," A Survey on Energy Efficient Multipath Routing In Wireless Sensor Network" International Journal of Computer Science and Information Technologies, Vol. 6 (1), 2015, 822-825.
2. Francesco Licandro, Alfio Lombardo, Giovanni Schembra" Multipath Routing and Rate-Controlled Video Encoding in Wireless Video Surveillance Networks

3. B. Krishnamoorthy, Y. Ginjali and C. E. Wills "On the Leakage of Personally Identifiable Information via Geosocial Networks" Comput. Comn Rev Vol 40 No 1pp, 112-117, 2010
4. Tootoonchian, S. Saroiou, Y. Ginjali and A. Wolman "Lockr-the Better Privacy for Social Networks", IEEE-2009 PP 1-12
5. B.C arbunar, M. Rahman, J. Ballestros, N. Rishe, "Towards Privacy Preserving Functionalities In Social Networking Approach"-intConf Mob Sec Approach 2013 Pp1-3
6. Foursquare, New York, NY, USA. (2014, Feb) [Online]. Available: https:// foursquare.com/
7. Yelp, Inc., San Francisco, CA, USA. (2014, Feb) [Online]. Available: http://www.yelp.com
8. E. Steel, G. Fowler (2010). Facebook in Privacy Breach [Online].Available: http://online.wsj.com/article/SB10001424052702304772804575558484075 2369%68.html