International Refereed Journal of Engineering and Science (IRJES)
ISSN (Online) 2319-183X, (Print) 2319-1821
Volume 3, Issue 11 (November 2014), PP.83-91

Interference Revelation in Mobile Ad-hoc Networks and Confrontation

A.Srinivas, (Assistant Professor)
G.Vasavi, (Associate Professor)
B.Kavitha Laxmi, (Assistant Professor)
K.Rama Krishna, (Assistant Professor)
Department of Computer Science Engineering & Technology

Abstract:- In this paper, we utilize the Several interference revelation techniques proposed for mobile ad hoc networks rely on each node passively monitoring the data forwarding by its next hop. This paper presents quantitative evaluations of false positives and their impact on monitoring based interference revelation for ad hoc networks. Experimental results show that, even for a simple three-node configuration, an actual ad-hoc network suffers from high false positives; these results are validated by Markov and probabilistic models. However, this false positive problem cannot be observed by simulating the same network using popular ad hoc network simulators, such as ns-2, OPNET or Glomosim. To remedy this, a probabilistic noise generator model is implemented in the Glomosim simulator. With this revised noise model, the simulated network exhibits the aggregate false positive behavior similar to that of the experimental tested. Simulations of larger (50-node) ad hoc networks indicate that monitoring-based interference revelation has very high false positives. These false positives can reduce the network performance or increase the overhead. In a simple monitoring-based system where no secondary and more accurate methods are used, the false positives impact the network performance in two ways: reduced throughput in normal networks without attackers and inability to mitigate the effect of attacks in networks with attackers.

Keywords:- quantitative evaluations , ad hoc network simulators , interference revelation, probabilistic analysis, monitoring-based interference , ad-hoc networks ,attacks, classic routing.

I. INTRODUCTION

A wireless ad-hoc network is a decentralized type of wireless network.[1] The network is ad hoc because it does not rely on a preexisting infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, and so the determination of which nodes forward data is made dynamically based on the network connectivity. In addition to the classic routing, ad hoc networks can use flooding for forwarding the data.

An ad hoc network typically refers to any set of networks where all devices have equal status on a network and are free to associate with any other ad hoc network devices in link range. Very often, ad hoc network refers to a mode of operation of IEEE 802.11 wireless networks .It also refers to a network device's ability to maintain link status information for any number of devices in a 1 link (aka "hop") range, and thus this is most often a Layer 2 activity. Because this is only a Layer 2 activity, ad hoc networks alone may not support a routable IP network environment without additional Layer 2 or Layer 3 capabilities.

→Application:

The decentralized nature of wireless ad-hoc networks makes them suitable for a variety of applications where central nodes can't be relied on, and may improve the scalability of wireless ad-hoc networks compared to wireless managed networks, though theoretical[2]and practical[3] limits to the overall capacity of such networks have been identified.

Minimal configuration and quick deployment make ad hoc networks suitable for emergency situations like natural disasters or military conflicts. The presence of dynamic and adaptive routing protocols enables ad-hoc networks to be formed quickly.

→Technical Requirements:

An ad-hoc network is made up of multiple “nodes” connected by “links". Links are influenced by the node's resources (e.g. transmitter power, computing power and memory) and by behavioral properties (e.g. reliability), as well as by link properties (e.g. length-of-link and signal loss, interference and noise). Since links can be connected or disconnected at any time, a functioning network must be able to cope with this dynamic

restructuring, preferably in a way that is timely, efficient, reliable, robust and scalable. The network must allow any two nodes to communicate, by relaying the information via other nodes. A "path" is a series of links that connects two nodes. Various routing methods use one or two paths between any two nodes; flooding methods use all or most of the available paths.

→Medium Access Control:
In most wireless ad hoc networks, the nodes compete for access to shared wireless medium, often resulting in collisions (interference). Using cooperative wireless communications improves immunity to interference by having the destination node combine self-interference and other-node interference to improve decoding of the desired signal.

→ 4G and Ad hoc Networking:

A major goal toward the 4G Wireless evolution is the providing of pervasive computing environments that can seamlessly and ubiquitously support users in accomplishing their tasks, in accessing information or communicating with other users at anytime, anywhere, and from any device. In this environment, computers get pushed further into background; computing power and network connectivity are embedded in virtually every device to bring computation to users, no matter where they are, or under what circumstances they work. These devices personalize themselves in our presence to find the information or software we need. The new trend is to help users in the tasks of everyday life by exploiting technologies and infrastructures hidden in the environment, without requiring any major change in the users behavior. This new philosophy is the basis of the Ambient Intelligence concept. The objective of ambient intelligence is the integration of digital devices and networks into the everyday environment, rendering accessible, through easy and ''natural'' interactions, a multitude of services and applications. Ambient intelligence places the user at the center of the information society. This view heavily relies on 4G wireless and mobile communications. There are two levels of integration. First is the integration of heterogeneous wireless networks with varying transmission characteristics such as Wireless LAN, WAN, PAN, as well as mobile ad hoc networks. At the second level we find the integration of wireless networks with the fixed network backbone infrastructure, the Internet, and PSTN. Much work remains to enable a seamless integration, for example that can extend IP to support mobile network devices. All IP Networks. 4G starts with the assumption that future networks will be entirely packet-switched, using protocols evolved from those in use in todays Internet . An all IP-based 4G wireless network has intrinsic advantages over its predecessors. IP is compatible with, and independent of, the actual radio access technology, this means that the core 4G network can be designed and evolves independently from access networks. Using IP based core network also means the immediate tapping of the rich protocol suites and services already available, for example, voice and data convergence, can be supported by using readily available VoIP set of protocols such as MEGACOP, MGCP, SIP, H.323, SCTP, etc. Finally the converged all-IP wireless core networks will be packet based and support packetized voice and multimedia on top of data.

II. SYSTEM OVERVIEW

The feasibility of the project is analyzed in this phase and business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis the feasibility study of the proposed system is to be carried out. This is to ensure that the proposed system is not a burden to the company. For feasibility analysis, some understanding of the major requirements for the system is essential.
Three key considerations involved in the feasibility analysis are

- Technical Feasibility
- Social Feasibility

→Technical Feasibility

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands on the available technical resources. This will lead to high demands being placed on the client. The developed system must have a modest requirement, as only minimal or null changes are required for implementing this system.

→Existing System:

In the existing work we've used several monitoring-based interference revelation techniques proposed in literature rely on each node passively monitoring the data forwarding by its next hop to mitigate packet dropping attacks by insider nodes. Though monitoring-based interference revelation is not likely to be accurate for ad hoc networks due to varying noise levels ,Varying signal propagation characteristics in different

directions, and interference from competing transmissions, there are no specific studies on the impact of noise on false positives and the impact of false positives on network Performance.

→Objective of the Proposed System

1 Interference revelation in heterogeneous WSNs by characterizing interference revelation with respect to the network parameters

2 Two revelation models

→Proposed System:

We proposed quantitative evaluations of false positives in monitoring-based interference revelation for Ad hoc networks. We showed that, even for a simple three-node configuration, an actual ad hoc network suffers from high false positives. We validated the experimental results using discrete-time Markov chains and probabilistic analysis. However, this problem of false positives cannot be observed by simulating the same three node network using popular ad hoc network simulators such as ns-2 with mobility extensions, OPNET or Glomosim, because they do not simulate the noise seen in actual network environments.

III. WORKING PRINCIPLE

About Manets: A mobile ad-hoc network (MANET) is a self-configuring infrastructure less network of mobile devices connected by wireless. *ad hoc* is Latin and means "for this purpose". Each device in a MANET is free to move independently in any direction, and will therefore change its links to other devices frequently. Each must forward traffic unrelated to its own use, and therefore be a router. The primary challenge in building a MANET is equipping each device to continuously maintain the information required to properly route traffic. Such networks may operate by themselves or may be connected to the larger Internet. MANETs are a kind of wireless ad hoc networks that usually has a routable networking environment on top of a Link Layer ad hoc network. The growth of laptops and 802.11/Wi-Fi wireless networking have made MANETs a popular research topic since the mid 1990s. Many academic papers evaluate protocols and their abilities, assuming varying degrees of mobility within a bounded space, usually with all nodes within a few hops of each other. Different protocols are then evaluated based on measure such as the packet drop rate, the overhead introduced by the routing protocol, end-to-end packet delays, network throughput etc.

In the next generation of wireless communication systems, there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes themselves, i.e., routing functionality will be incorporated into mobile nodes.

A mobile ad hoc network (MANET) is a collection of wireless devices moving in seemingly random directions and communicating with one another without the aid of an established infrastructure. To extend the reach ability of a node, the other nodes in the network act as routers. Thus, the communication may be via multiple intermediate nodes between source and destination. Since MANETs can be set up easily and inexpensively, they have a wide range of applications, especially in military operations and emergency and disaster relief efforts. In a MANET, the users mobile devices are the network, and they must cooperatively provide the functionality usually provided by the network infrastructure (e.g., routers, switches, servers). In a MANET, no infrastructure is required to enable information exchange among users mobile devices. We can envisage these devices as an evolution of current mobile phones, and emerging Pads equipped with wireless interfaces.

Security Issues In MANETS:

In recent years mobile ad hoc networks (MANETs) have received tremendous attention because of their self- configuration and self-maintenance capabilities. While early research effort assumed a friendly and cooperative environment and focused on problems such as wireless channel access and multichip routing, security has become a primary concern in order to provide protected communication between nodes in a potentially hostile environment. Although security has long been an active research topic in wire line networks, the unique characteristics of MANETs present a new set of nontrivial confrontation to security design. These confrontation include open network architecture, shared wireless medium, stringent resource constraints, and highly dynamic network topology. Consequently, the existing security solutions for wired networks do not directly apply to the MANET domain. The ultimate goal of the security solutions for MANETs is to provide

security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. In order to achieve this goal, the security solution should provide complete protection spanning the entire protocol stack.

Layer: Security issues:
Application layer: Detecting and preventing viruses, worms, malicious codes, and application abuses.
Transport layer: Authenticating and securing end-to-end communications through data encryption.
Network layer: Protecting the ad hoc routing and forwarding protocols.
Link layer: Protecting the wireless MAC protocol and providing link-layer security support.
Physical layer: Preventing signal jamming denial-of-service attacks

→Attacks:

A MANET provides network connectivity between mobile nodes over potentially multi hop wireless channels mainly through link-layer protocols that ensure one-hop connectivity, and network-layer protocols that extend the connectivity. to multiple hops. These distributed protocols typically assume that all nodes are cooperative in the coordination process. This assumption is unfortunately not true in a hostile environment .Because cooperation is assumed but not enforced in MANETs, malicious attackers can easily disrupt network operations by violating protocol specifications. The main network-layer operations in MANETs are ad hoc routing and data packet forwarding, which interact with each other and fulfill the functionality of delivering packets from the source to the destination.

The ad hoc routing protocols exchange routing messages between nodes and maintain routing states at each node accordingly. Based on the routing states, data packets are forwarded by intermediate nodes along an established route to the destination. Nevertheless, both routing and packet forwarding operations are vulnerable to malicious attacks, leading to various types of malfunction in the network layer. While a comprehensive enumeration of the attacks is out of our scope, such network-layer vulnerabilities generally fall into one of two categories: routing attacks and packet forwarding attacks, based on the target operation of the attacks. The family of routing attacks refers to any action of advertising routing updates that does not follow the specifications of the routing protocol. The specific attack behaviors are related to the routing protocol used by the MANET. For example, in the context of DSR , the attacker may modify the source route listed in the RREQ or RREP packets by deleting a node from the list, switching the order of nodes in the list, or appending a new node into the list . When distance-vector routing protocols such as AODV are used, the attacker may advertise a route with a smaller distance metric than its actual distance to the destination, or advertise routing updates with a large sequence number and invalidate all the routing updates from other nodes . By attacking the routing protocols, the attackers can attract traffic toward certain destinations in the nodes under their control, and cause the packets to be forwarded along a route that is not optimal or even nonexistent. The attackers can create routing loops in the network, and introduce severe network congestion and channel contention in certain areas. Multiple colluding attackers may even prevent a source node from finding any route to the destination, and partition the network in the worst case.

There are still active research efforts in identifying and defeating more sophisticated and subtle routing attacks. For example, the attacker may further subvert existing nodes in the network, or fabricate its identity and impersonate another legitimate node. A pair of attacker nodes may create a wormhole and shortcut the normal flows between each other. In the context of on-demand ad hoc routing protocols, the attackers may target the route maintenance process and advertise that an operational link is broken. In addition to routing attacks, the adversary may launch attacks against packet forwarding operations as well. Such attacks do not disrupt the routing protocol and poison the routing states at each node. Instead, they cause the data packets to be delivered in a way that is intentionally inconsistent with the routing states. For example, the attacker along an established route may drop the packets, modify the content of the packets, or duplicate the packets it has already forwarded.

Another type of packet forwarding attack is the denial-of-service (DoS) attack via network-layer packet blasting, in which the attacker injects a large amount of junk packets into the network. These packets waste a significant portion of the network resources, and introduce severe wireless channel contention and network congestion in the MANET. Recent research efforts have also identified the vulnerabilities of the link-layer protocols, especially the de facto standard IEEE 802.11 MAC protocol [3], for MANETs. It is well known that 802.11 WEP is vulnerable to several types of cryptography attacks due to the misuse of the cryptographic primitives . The 802.11 protocol is also vulnerable to Do's attacks targeting its channel contention and reservation schemes. The attacker may exploit its binary exponential back off scheme to deny access to the wireless channel from its local neighbors. Because the last winner is always favored among local contending nodes, a continuously transmitting node can always capture the channel and cause other nodes to back off endlessly. Moreover, bakeoffs at the link layer can incur a chain reaction in upper layer protocols using back off schemes (e.g., TCP's window management). Another vulnerability of 802.11 comes from the NAV field carried

in the request to send/clear to send (RTS/CTS) frames, which indicates the duration of channel reservation. An adversarial neighbor of either the sender or the receiver may overhear the NAV information and then intentionally introduce a 1-bit error into the victim's link-layer frame by wireless interference. The corrupted frame has to be discarded by the receiver after error detection. This effectively constitutes another type of DoS attack.

→ Modules Specifications:

Module1: In this module, we are going to connect the network .Each node is connected the neighboring node and it is independently deployed in network area. And also deploy the each port no is authorized in a node.

Module-2: In this module, browse and select the source file. And selected data is converted into fixed size of packets. And the packet is send from source to detector.

Module-3: The interference revelation is defined as a mechanism for a WSN to detect the existence of inappropriate, incorrect, or anomalous moving attackers. In this module check whether the path is authorized or unauthorized. If path is authorized the packet is send to valid destination. Otherwise the packet will be deleted. According port no only we are going to find the path is authorized or Unauthorized.

Module-4: If the packet is received from other than the port no it will be filtered and discarded. This filter only removes the unauthorized packets and authorized packets send to destination.

Module-5: In this module, after filtering the invalid packets all the valid Packets will reach the destination.

System Design

The most creative and challenging phase of the life cycle is system design. The term design describes a final system and the process by which it is developed. It refers to the technical specifications that will be applied in implementations of the candidate system. The design may be defined as "the process of applying various techniques and principles for the purpose of defining a device, a process or a system with sufficient details to permit its physical realization".

→Use case Diagrams represent the functionality of the system from a user's point of view. Use cases are used during requirements elicitation and analysis to represent the functionality of the system. Use cases focus on the behavior of the system from external point of view.

Actors are external entities that interact with the system. Examples of actors include users like administrator, bank customer …etc., or another system like central database.

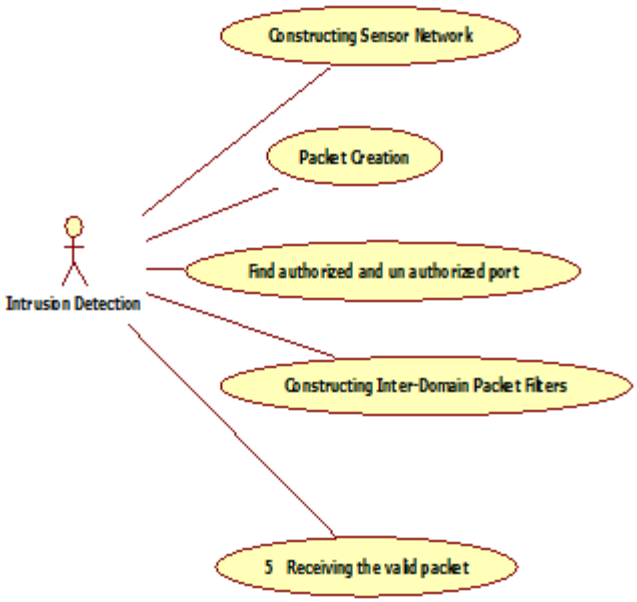

Fig: Use-Case Diagram

IV. Implementation of System

Java Packages and api:

→AWT

The AWT classes contained by the java.awt package. It is one of the largest packages. Because it is logically organized in a top-down, hierarchical fashion, it is easier to understand and use than you might at first

believe. AWT contains numerous classes and methods that allow you to create and manage windows. It also explains further aspects of of java's event handling mechanism. The main purpose of the AWT is to support applet windows, it can be used to create stand –alone windows that run in a GUI environment such as windows.

→ Applet

The applet class is contained by the java.applet package. Applet contains several methods that give you detailed control over the execution of your applet. Java.applet also defines three interfaces AppletContext, AudioClip, AppletStub. All applet must import with java.applet .applets must also import with the java.awt.

→Util

The java util package contains some of the most exiting enhancements added by java 2 collections .a collections is group of objects the addition of collections caused fundamental alterations in the structure and architecture of many elements of java.util.java.util contains a wide range of functionality.thease classes and interfaces are used throughout core java packages. These include classes that tokenize the string, work with dates, compute random numbers and observe events.

→Net:

The java.net package which provides support of networking. Java is good language for networking the classes are defined in java.net package. These networking classes encapsulate the "socket" paradigm pioneered by the BSD.

→Zip

The java.util.zip package provides the ability to read and write files in the popular ZIP and GZIP formats. Both ZIP and GZIP input and output streams are available. Other classes implement the ZLIB algorithms for compression and decompression.

→Swing

The swing is a set of classes that provides more powerful and flexible components than are possible with the AWT. Unlike AWT components Swing components are not implemented by platform specific code. They are written entirely in java and, therefore, are platform-independent. The term lightweight is used to describe such elements. The number of classes and interfaces in the swing packages is substantial. Swing is area that you will want to explore further on your own

- Application Programming Interfaces

Listeners are created by implementing one or more of the interfaces Defined by the java.awt.event package. When an event occurs, the event Source invokes the appropriate method defined by the listener.

- Action Listener interface

This interface defines the actionPerformed () method that is Invoked when an action event occurs. Its general form is shown void actionPerformed (ActionEvent ae)

→Basic Foundation Classes

Applet

Applet provides all necessary support for execution, such as starting and stoping.it also provides methods that load and display images and methods that load and play audio clips. Applet extends the AWT class panel. In turn panel extends container, which extends component. These classes provide support java's window based, graphical interface. Thus applet provides all of the necessary support for window-based activities.

Image:This class provides support for imaging. Images are objects of the Image class, which is a part of the java.awt package. There are a large number of imaging classes and interfaces defined by java.awt.image and its not possible to examine them all.

→Event: The classes that represent events are at the core of java's events handling mechanisms. They provide a consistent, easy-to-use means of encapsulating events. At the root of the java event class hierarchy is Event Object, which is in java.util. it is the super class for all events. Its one

constructor is shown Event Object (Object src)

Sample Source Coding:

```
import java.awt.*;
import java.awt.event.*;
import javax.swing.*;
```

```
import java.io.*;
import java.net.*;
/*** Summary description for Source*
 public class Source extends JFrame
{
	// Variables declaration
	private JLabel jLabel1;
	private JLabel jLabel2;
	private JLabel jLabel3;
	private JTextField jTextField1;
	private JComboBox jComboBox1;
	private JTextArea jTextArea1;
	private JScrollPane jScrollPane1;
	private JButton jButton1;
	private JButton jButton2;
	private JButton jButton3;
	private JPanel contentPane;
	String msg="";
	int flag=1;
	int flag1=1;
	Socket n1_client;
	String destination;
	int limit;
	String a[]={"Select","R-101","R-102","R-103","I-104"};
	int len;
	int packets;
	int rem;
	// End of variables declaration
	public Source()
	{
		super();
		initializeComponent();
		//
		// TODO: Add any constructor code after initializeComponent call
		//
		this.setVisible(true);
	}
	/**
	 * This method is called from within the constructor to initialize the form.
	 * WARNING: Do NOT modify this code. The content of this method is always regenerated
	 * by the Windows Form Designer. Otherwise, retrieving design might not work properly.
	 * Tip: If you must revise this method, please backup this GUI file for JFrameBuilder
	 * to retrieve your design properly in future, before revising this method.
	 */
	private void initializeComponent()
	{
		jLabel1 = new JLabel();
		jLabel2 = new JLabel();
		jLabel3 = new JLabel();
		jTextField1 = new JTextField();
		jComboBox1 = new JComboBox(a);
		jTextArea1 = new JTextArea();
		jScrollPane1 = new JScrollPane();
		jButton1 = new JButton();
		jButton2 = new JButton();
		jButton3 = new JButton();
		contentPane = (JPanel)this.getContentPane();

		//
```

```
        // jLabel1
        //
        jLabel1.setText("INTERFERENCE DETECTION");
        //
        // jLabel2                  //
        jLabel2.setText("Port No");
        //
        // jLabel3                  //
        jLabel3.setText("Status Information");
        //
        // jTextField1
        //
        jTextField1.addActionListener(new ActionListener() {
                public void actionPerformed(ActionEvent e)
                {
                        jTextField1_actionPerformed(e);
                }

        });
        //
        // jComboBox1
        //
        jComboBox1.addActionListener(new ActionListener() {
                public void actionPerformed(ActionEvent e)
                {
                        jComboBox1_actionPerformed(e);
                }
        });             //
        // jTextArea1           //
        //
        // jScrollPane1         //
jScrollPane1.setViewportView(jTextArea1);
        //
        // jButton1             //
        jButton1.setBackground(new Color(255, 255, 255));
        jButton1.setText("Browse");
        jButton1.addActionListener(new ActionListener() {
                public void actionPerformed(ActionEvent e)
                {
                jButton1_actionPerformed(e);
                }
        });
```

V. CONCLUSION

Several monitoring-based interference revelation techniques proposed in literature rely on each node passively monitoring the data forwarding by its next hop to mitigate packet dropping attacks by insider nodes. Though monitoring-based interference revelation is not likely to be accurate for ad hoc networks due to varying noise levels, varying signal propagation characteristics in different directions, and interference from competing transmissions , there are no specific studies on the impact of noise on false positives and the impact of false positives on network performance. In this paper, we presented quantitative evaluations of false positives in monitoring-based interference revelation for ad hoc networks. We showed that, even for a simple three node configuration, an actual ad hoc network suffers from high false positives.

VI. FUTURE ENHANCEMENTS

Our Future enhancements are interference detections in internet application and parallel computer interconnection network.

REFERENCES

[1]. B. Awerbuch, D. Holmer, C. Nita-Rotaru, and H. Rubens, "An On-Demand Secure Routing Protocol Resilient to Byzantine Failures," Proc. ACM WiSe, pp. 21-30, Sept. 2002.

[2]. S. Bansal and M. Baker, "Observation-Based Cooperation Enforcement in Ad Hoc Networks," Research Report cs. NI/0307012,Standford Univ., 2003.

[3]. R.V. Boppana and X. Su, "An Analysis of Monitoring Based Interference Revelation for Ad Hoc Networks," Proc. IEEE Globecom: Computer and Comm. Network Security Symp., Dec. 2008.

[4]. R.V. Boppana and S. Desilva, "Evaluation of a Stastical Technique to Mitigate Malicious Control Packets in Ad Hoc Networks," Proc.Int'l Symp. World of Wireless Mobile and Multimedia Networks (WoWMoM)/Workshop Advanced Experimental Activities on Wireless Networks and Systems, pp. 559-563, 2006.

[5]. S. Buchegger and J.Y. Le Boudec, "A Robust Reputation System for Mobile Ad-Hoc Networks," Proc. Workshop Economics of Peerto-Peer Systems (P2PE '04), 2004.

[6]. S. Buchegger, C. Tissieres, and J.Y. Le Boudec, "A Test-Bed for Misbehavior Revelation in Mobile Ad-Hoc Networks – How Much Can Watchdogs Really Do?" Proc. IEEE Workshop Mobile Computing Systems and Applications (WMCSA '04), 2004.

[7]. S. Buchegger and J.-Y. Le Boudec, "Performance Analysis of the Confidant Protocol: Cooperation of Nodes Fairness in Dynamic Ad-Hoc Networks," Proc. IEEE/ACM MobiHoc, 2002.

[8]. R. Burchfield, E. Nourbakhsh, J. Dix, K. Sahu, S. Venkatesan, and R. Prakash, "RF in the Jungle: Effect of Environment Assumptions on Wireless Experiment Repeatability," Proc. IEEE Int'l Conf.Comm. (ICC '09), pp. 1-6, 2009.

[9]. I. Chlamtac, M. Conti, and J.J.-N. Liu, "Mobile Ad Hoc Networking:Imperatives and Challenges," Ad Hoc Networks, vol. 1, no. 1,pp. 13-64, 2003.

[10]. Cisco Systems Inc., Linksys WRT54G v2.2 Wireless-G Broadband Router, http://www.linksys.com, 2004.

[11]. L. Eschenauer, V.D. Gligor, and J. Baras, "On Trust Establishment in Mobile Ad-Hoc Networks," Proc. Security Protocols, pp. 47-66, 2003.

[12]. J. Hu, "Cooperation in Mobile Ad Hoc Networks," Technical Report TR-050111, Dept. of Computer Science, Florida State Univ., 2005.

Author Details:

Mr. A. Srinivas received Master of Technology in Computer Science Engineering from Jawaharlal Nehru Technological University Hyderabad in 2009. His research interests include Cloud Computing, Data Mining, Information Security, Software Testing, Wireless Networks and Software Quality. He is currently working as an Assistant Professor, Department of Computer Science & Engineering in Holy Mary Institute of Technology and Science (HITSCOE), (V) Bogaram, (M) Keesara, R.R.Dist, Telangana, India.

G.Vasavi, she is currently working as an Associate Professor, Department of Computer Science &Engineering in HITAM, Hyderabad, R.R.Dist, and Telangana, India. She received the master of technology degree in Jawaharlal Nehru Technological University Hyderabad, India. She Has 8+ Years Teaching Experience. Research Interests Include mobile ad-hoc networks, Network security, Algorithms.

B.Kavitha Laxmi, she is currently working as an Assistant Professor, Department of Computer Science &Engineering in HITAM, Hyderabad, R.R.Dist, Telangana, India. she received the master of technology degree in VNR Vignana Jyothi Institute of Engineering and Technology- Jawaharlal Nehru Technological University Hyderabad, India in 2010. She Has 5+ Years Teaching Experience. Research Interests Include mobile ad-hoc networks, Data Mining, Web Technologies Cloud Computing and data warehouse.

Mr.K.Ramakrishna, presently working as an assistant professor in computer science engineering and technology department, Samara University, samara, Ethiopia .He received the master of technology degree in VNR Vignana Jyothi Institute of Engineering and Technology- Jawaharlal Nehru Technological University Hyderabad, India in 2010. He received the bachelor of technology degree in The Vazir Sultan College of Engineering and technology, kakatiya university, Warangal, India. He Has 6+ Years Teaching Experience, His Research Interests Include mobile ad-hoc networks, Data Mining, Information Security, Software Testing, mobile communication and cloud computing.