A Survey on Intrusion in Ad Hoc Networks and its Detection Measures

Ms. Preetee K. Karmore

Department of Computer Science & Engineering
G. H. Raisoni College of Engineering
Nagpur, India.

Ms. Sonali T. Bodkhe

Department of Computer Science & Engineering
G. H. Raisoni College of Engineering
Nagpur, India.

Abstract—Ad hoc wireless networks are defined as the category of wireless networks that utilizes multi-hop radio relaying and are capable of operating without the support of any fixed infrastructure hence, they are called infrastructure less networks. The lack of any central coordination makes them more vulnerable to attacks than wired networks. Due to some unique characteristics of MANETs, prevention methods alone are not sufficient to make them secure therefore, detection should be added as another defense before an attacker can breach the system. Network intrusion detection is the process of monitoring the events occurring in the network and analyzing them for signs of intrusions, defined as attempts to compromise the confidentiality. In this paper, we define and discuss various techniques of Intrusion Detection. We also present a description of routing protocols and types of security attacks possible in the network.

Keywords- Intrusion detection system; Ad hoc network; Attacks; Network Security.

I. INTRODUCTION

A mobile ad hoc network (MANET) is a self-configuring network that is formed automatically by a collection of mobile nodes without the help of a fixed infrastructure or centralized management. Each node communicates with other node in its radio communication range by using wireless transmitter and receiver which is equipped on each node. Each node cooperates for transmitting packets to a node that is out of its radio range, this is known as multi-hop communication. Therefore, each node must act as both a host and a router at the same time.

The dynamic and cooperative nature of ad-hoc networking without a centralized authority for authentication and monitoring is susceptible to attacks that breaks down or exploit the cooperative behavior of the ad-hoc routing. Attacks can come in the form of a passive attack or an active attack targeted at various layers of the Open System Interconnect (OSI) model.

Therefore, intrusion detection may be more suitable for wireless networks. Intrusion detection is defined as the method to identify “any set of actions that attempt to compromise the integrity, confidentiality, or availability of a resource” [15]. An intrusion detection system analyzes network or system activities captured in audit data and uses patterns of well known attacks or normal profile to detect potential attacks. Intrusion detection is used in the networks by comparing the set of baselines of the system with the present behavior of the system [5]. Thus, a basic assumption is that the normal and abnormal behaviors of the system can be characterized [1].

Intrusion detection is one of key techniques behind protecting a network against intruders. An Intrusion Detection System tries to detect and alert on attempted intrusions into a system or network, where an intrusion is considered to be any unauthorized or unwanted activity on that system or network [13].

There are two basic techniques of intrusion detection: misuse detection and anomaly detection. [8]. Misuse detection uses the “signatures” of known attacks [12]. Misuse detection is to collect information, then match it with the known intrusion pattern. The advantage of misuse detection system is the burden on small, high rate of detection accuracy, 95% of the intrusion detection products are based on the misuse detection, but the weakness of this method is not found in unknown attacks, needing to constantly upgrade [3]. In anomaly detection, profiles of normal behavior of systems, usually established through automated training, are compared with the actual activity of the system to flag any significant deviation. The disadvantage of this approach is that loss detecting rate and false detection rate of intrusion detection is very high. [12].

The paper is focused on the detailed study of vulnerabilities in ad hoc networks which affects intrusion detection, attacks possible on ad hoc networks with a brief overview and different methods of intrusion detection.

II. VULNERABILITIES OF AD HOC NETWORK

Vulnerabilities in ad hoc network described in [6, 10, 11 and 7] are:

1. Dynamic topology: Due to dynamic topology, ad hoc networks require sophisticated routing protocols. A particular difficulty is that misbehaving node can generate wrong routing information which is hard to discover. Mobility of devices also creates a problem.

2. Absence of infrastructure: Ad hoc networks do not have any fixed infrastructure which makes traditional security mechanism of cryptography and certification inapplicable.

3. Vulnerability of nodes: Physical protection of nodes is not possible hence they can more easily be captured and falls under the control of an attacker.

4. Lack of Secure Boundaries: The meaning of this vulnerability is self-evident: there is not such a clear secure boundary in the mobile ad hoc network, which can be compared with the clear line of defense in the traditional wired network. This vulnerability originates from the nature of the mobile ad hoc network: freedom to join, leave and move inside the network.

III. ROUTING PROTOCOLS IN MANET

Routing protocols between any pair of nodes within an ad hoc network can be difficult because the nodes can move randomly and can also join or leave the network. This means that an optimal route at a certain time may not work seconds later. Following are protocols that are used in MANET:

A. Dynamic source Routing Protocol

DSR uses source routing to deliver packets through MANET. That is, the sender of a data packet finds a source route (i.e., a full path from the sender to the receiver) and includes it in the packet header [17]. The intermediate nodes use this information to determine whether they should accept a packet and where to forward it. The protocol operates on two mechanisms: route discovery and route maintenance.

Route discovery: Route discovery is used when the packet sender has not yet known the correct path to the packet destination. It works by broadcasting a ROUTE REQUEST message throughout the network in a controlled manner until it is answered by a ROUTE REPLY message from either the destination itself or an intermediate node that knows a valid path to it. For better performance, the source and intermediate routes save the route information in cache for future use. Furthermore, intermediate nodes can also learn new routes by eavesdropping to other route discovery messages taken place in the neighborhood.

Route maintenance: Finally, route maintenance mechanism is used to notify source and potentially trigger new route discovery events when changes in the network topology invalidate a cached route.

B. Ad Hoc on-Demand Distance Vector Routing Protocol

ADHOC on Demand Distance Vector Routing (AODV) is an improvement of Destination sequenced distance vector routing (DSDV) as it minimizes the number of required broadcasts since it creates routes in an on-demand basis, in contrast to Destination Sequenced Distance Vector routing (DSDV) which maintains a complete set of routes [3]. Ad hoc On-demand Distance Vector Routing Protocol uses an on demand approach for finding routes, that is, a route is established only when it is required by a source node for transmitting data packets. It employs destination sequence numbers to identify the most recent path.

The major difference between AODV and DSR is that DSR uses source routing in which a data packet carry complete route to be traversed. However, in AODV source node and intermediate node store the next hop information corresponding to each flow, for data packet transmission. The Major difference between AODV and other on demand routing protocols is that it uses a destination sequence number to determine up-to-date path to the destination. A node updates its path information only if the DestSeqNum of the current packet received is greater than the last DestSeqNum stored at the node. A route request carries the source identifier (SrcId), the destination identifier (DestId), the source sequence number (SrcSeqNum), the destination sequence number

(DestSeqNum), the broadcast identifier (BcastId) and time to live (TTL) field. DestSeqNum indicates the freshness of the route that is accepted by the source. When an intermediate node receives a RouteRequest, it either forwards it or prepares a RouteReply if it has a valid route to the destination. The validity of the route at intermediate node is determined by comparing the sequence number at the intermediate node with the destination sequence number in the routerequest packet. If a routerequest is received multiple times, which is indicated by BcastId-SrcId pair, the duplicate copies are discarded.

All intermediate nodes having valid routes to the destination, or the destination nodes itself are allowed to send RouteReply packets to the source. Every intermediate node, while forwarding a RouteRequest enters the previous node address and it's BroadcastId. A timer is used to delete this entry in case a RouteReply is not received before timer expires. This helps in storing active path at the intermediate node as AODV does not employ source routing of data packets. When a node receives a RouteReply packet, information about the previous node from which the packet was received is also stored in order to forward the data packet to this next node as the next hop toward the destination.

C. Temporally Ordered Routing Algorithm

TORA uses a metric referred to as the "height" of the node to assign a direction to links for forwarding packets to a given destination. The node heights can be totally ordered lexicographically, and thus define a directed acyclic graph rooted at the destination.

The TORA attempts to achieve a high degree of scalability using a "flat", non-hierarchical routing algorithm. In its operation the algorithm attempts to suppress, to the greatest extent possible, the generation of far-reaching control message propagation. In order to achieve this, the TORA does not use a shortest path solution, an approach which is unusual for routing algorithms of this type.

TORA builds and maintains a Directed Acyclic Graph rooted at a destination. No three nodes may have the same height. Information may flow from nodes with higher heights to nodes with lower heights. Information can therefore be thought of as a fluid that may only flow downhill. By maintaining a set of totally-ordered heights at all times, TORA achieves loop-free multipath routing, as information cannot 'flow uphill' and so cross back on itself. There are three functions: creating routes, maintaining routes and erasing routes.

Creating routes: Creating routes is performed on demand using a query/replay process.

Maintaining routes: When a node loses its last downstream link the algorithm reorients the directed acyclic graph such that all downstream paths lead to the destination.

Re-optimization of routes: TORA does not compute the shortest path: paths may be suboptimal. It starts close to optimal and tends to "loosen", as it reacts to topological changes. A secondary mechanism, not tied to the rate of topological change, is used to re-optimize routes. During the route creation and maintenance phases, nodes use a height metric to establish a directed acyclic graph (DAG) rooted at destination. Thereafter links are assigned based on the relative height metric of neighboring nodes. During the times of mobility the DAG is broken and the route maintenance unit comes into picture to reestablish a DAG routed at the destination.

IV. ATTACKS ON MOBILE AD HOC NETWORKS

Attacks on mobile ad hoc networks can be classified into following two categories:

Passive Attacks: A passive attack does not disrupt proper operation of the network. The attacker snoops the data exchanged in the network without altering it.

Active Attacks: An active attack attempts to alter or destroy the data being exchanged in the network, thereby disrupting the normal functioning of the network. It can be classified into two categories external attacks and internal attacks [9]. External attacks are carried out by nodes that do not belong to the network. These attacks can be prevented by using standard security mechanisms such as encryption techniques and firewalls. Internal attacks are carried out by compromised nodes that are actually part of the network [9]. Next we present some types of active attacks that can usually be easily performed against an ad hoc network.

A. *Blackhole Attack*

Black holes refer to places in the network where incoming traffic is silently discarded (or "dropped"), without informing the source that the data did not reach its intended recipient. In this attack, an attacker or malicious node uses the routing protocol to advertise itself as having the shortest path to the node whose packets it wants to intercept [9].

An attacker listen the requests for routes in a flooding based protocol. When the attacker receives a request for a route to the destination node, it creates a false reply consisting of an extremely short route. If the malicious reply reaches the source node before the reply from the actual node, a fake route gets created [9].

When the malicious node present between two communicating nodes, it can do anything with the packets passing between them, either it can drop the packets or it will not further forward the packets.

For example in fig 1[9], source node S wants to send data packets to the destination node D, it will initiate route discovery process to find route from S to D. Suppose node 2 is malicious node. Whenever node 2 receive route request message it will immediately reply to the source with route consisting of extremely short route. If the reply from node 2 reaches first to the source, it will think that the process of route discovery has been finished and it will ignore all the reply messages from other nodes and begins to send data packets to node 2. As a result, all packets through the malicious node is consumed or lost.

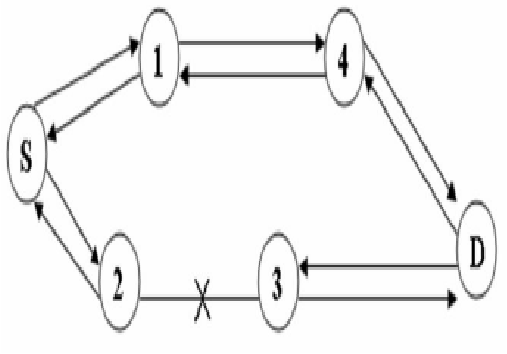

Fig 1: Black hole attack

B. Routing table overflow

In a routing table overflow attack the attacker attempts to create routes to nonexistent nodes. The goal is to create enough routes to prevent new routes from being created or to overwhelm the protocol implementation [14].

C. Wormhole Attack

A wormhole attack is composed of two attackers and a wormhole tunnel. To establish a wormhole attack, attackers create a direct link, referred to as a wormhole tunnel, between them. Wormhole tunnels can be established by means of a wired link, a high quality wireless out-of-band link or a logical link via packet encapsulation. After building a wormhole tunnel, one attacker receives and copies packets from its neighbors, and forwards them to the other colluding attacker through the wormhole tunnel. This latter node receives these tunneled packets and replays them into the network in its vicinity. Wormhole attacks are relatively easy to deploy but may cause great damage to the network [16].

D. Denial of Service (DoS)

Denial of service attack, aims to crab the availability of certain node or even the services of the entire ad hoc networks. Denial of service attack, aims to crab the availability of certain node or even the services of the entire ad hoc networks. In the traditional wired network, the DoS attacks are carried out by flooding some kind of network traffic to the target so as to exhaust the processing power of the target and make the services provided by the target become unavailable. Nevertheless, it becomes not practical to perform the traditional DoS attacks in the mobile ad hoc networks because of the distributed nature of the services. Moreover, the mobile ad hoc networks are more vulnerable than the wired networks because of the interference-prone radio channel and the limited battery power. In the practice, the attackers exactly use the radio jamming and battery exhaustion methods to conduct DoS attacks to the mobile ad hoc networks, which well correspond to the two vulnerabilities: Impersonation and Eavesdropping [9].

E. Eavesdropping

This attack aims to obtain some confidential information that should be kept secret during the communication. Confidential information is nothing but the location, public key, private key or even passwords of the nodes. As this information is very important for security purpose, this must be kept away from unauthorized access. This attack usually happens in the mobile ad hoc networks.

F. Traffic Analysis & Monitoring

Traffic analysis attack adversaries monitor packet transmission to infer important information such as a source, destination, and source-destination pair.

V. SECURITY SCHMES IN THE MOBILE AD HOC NETWORKS

There are many different schemes which are used to secure the Mobile ad hoc network. Some of these are discussed below:

A. Intrusion Detection Tecgniques in MANET

1) Profile Based Intrusion Detection Approach

R. Saminatha [2] proposed profile based approach. In this approach, each node monitors its neighbor traffic and builds a profile for each of its neighbors. The profile includes all the features as shown in Table 1[2]. This profile is used as a threshold to detect intrusion. Mean and standard deviation are calculated for each sample of data. The set of upper and lower bound values for the anomaly has to be prepared. Once the traffic feature exceeds the threshold, an alert should be produced. The node can use the profile to monitor the neighboring node's behavior as shown in Figure 2 [2].

TABLE1: TRAFFIC RELATED FEATURES

Dimention	**Values**
Packet type	Data, route(all),ROUTE REQUEST, ROUTE REPLY, ROUTE ERROR and HELLO message
Flow direction	Received, sent, forwarded and dropped
Statistic measures	Count the average and standard deviation of Number of packets or size of data packets.

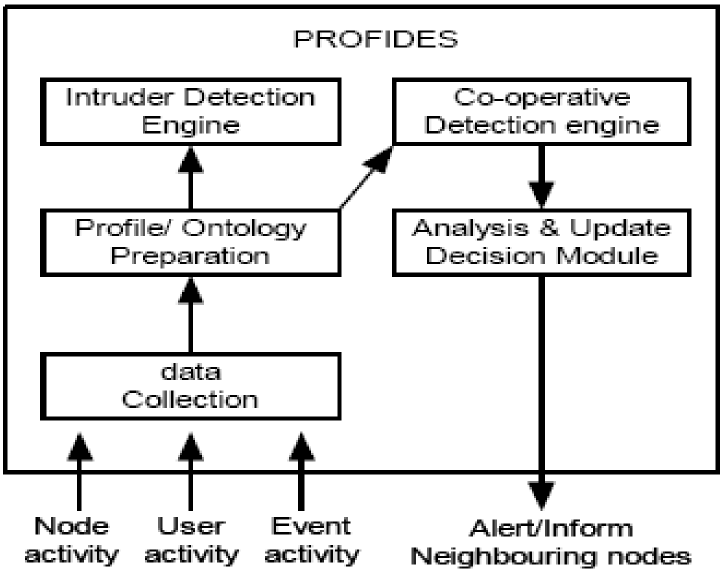
PROFIDES
Intruder Detection Engine
Co-operative Detection engine
Profile/ Ontology Preparation
Analysis & Update Decision Module
data Collection
Node activity
User activity
Event activity
Alert/Inform Neighbouring nodes

Figure 2: Profile Based Intrusion Detection Process

2) The Enhancement of Intrusion Detection System for Ad Hoc Network (EIDAN)

In [5] L. Prema Rajeswari proposed an architecture model for intrusion detection. The Enhancement of Intrusion Detection System for ADHOC Network (EIDAN) is a host-based network intrusion detection system. EIDAN system is designed to detect three types of attacks i. e. resource consumption attack, packet dropping attack, fabrication attack. The logical component of this architecture is shown in fig 3 [5].

1. **Traffic interception module:**

This module captures the incoming traffic from the network and selects which of these packets should be further processed. Once path has established then by receiving each packet has traced by Enhancement of Intrusion Detection (EIDAN) System has to check the node information already present in the routing table entry .If condition not satisfied then packet is picked for further process.

2. **Event generation module:**

This module is responsible for abstracting the essential information required for the attack analysis module to find whether there is malicious activity in the network. Sequence number, time, IP address of the node, hop count, packet size, such kind of information is extracted.

3. **Attack analysis:**

This module analyses any defined attacks are to found are not, if it is found then send malicious packet to counter measure module to take appropriate action. Attack analysis module can only verify type of attack.

4. **Counter measure module:**

The final module of the architecture is the countermeasure module, which is responsible for taking action to drop malicious packet received from the attack analysis module. Therefore, the Enhancement of Intrusion Detection System for ADHOC Network (EIDAN) intrusion detection component operates between the network traffic and the routing protocol, that require no modifications to the routing protocol that is utilized in the network.

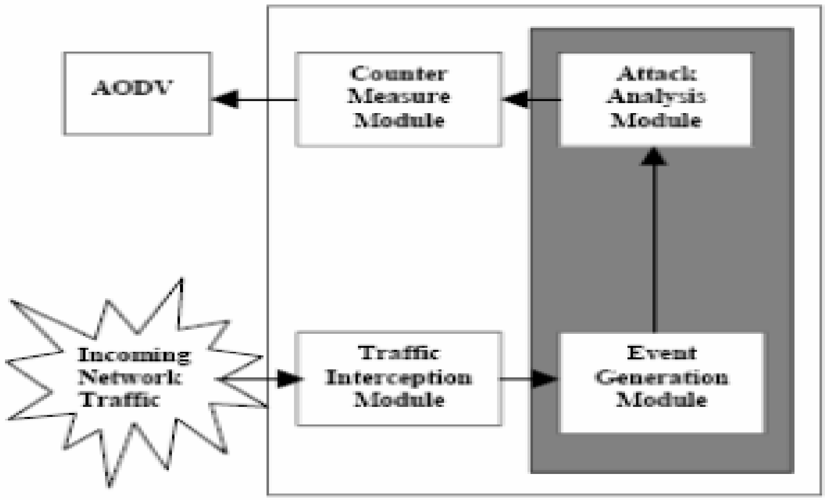

Fig 3: Enhancement of Intrusion Detection System for ADHOC Networks

3) Agent Based Efficient Anomaly Intrusion Detection System in ad hoc networks

This approach has been used to address security problems related to attacks in a wireless networks which is entirely based on anomaly based method. R. Nakkeeran [1] incorporates new technique such as mining and agents to provide solutions against wireless networks. It provides three different techniques to provide suffice security solution to current node, Neighboring Node and Global networks.

1. It monitors its own system and its environment dynamically. It uses classifier construction to find out the local anomaly.

2. Whenever the node want to transfer the information from the node F to B, it broadcast the message to E and A. before it sends the message, it gathers the neighboring nodes (E &B) information using mobile agent. It calls the classifier rule to find out the attacks with help of test train data.

3. It provides same type of solution throughout the global networks. Figure 4 and 5 [1] shows the architecture of the system to prevent the attacks in wireless networks.

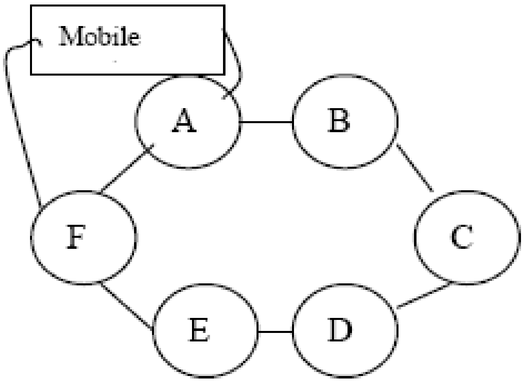

Fig 4: System Architecture Outlines

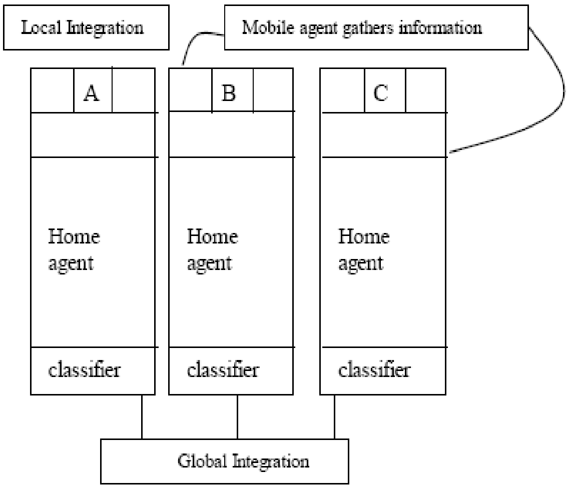

Fig 5: Agent based cooperative and distributive System Architecture

4) Intrusion Detection based on K-means clustering

In [16] Meng Jianliang said that Clustering is the method of grouping objects into meaningful subclasses so that the members from the same cluster are quite similar, and the members from different clusters are quite different from each other. In this paper author used k-means clustering algorithm for detection of intrusion in the network. The method is evaluated over the KDD Cup 1999 data, which contains a wide variety of intrusions simulated in a military network environment [16]. Each sample in the data is a record of extracted features from a network connection gathered during the simulated intrusions. It consist of TCP connection related features like number of bytes transferred, protocol type, domain specific features as number of file creation, number of failed login attempts, and whether root shell was obtained [16]. Experimental results on a subset of KDD-99 dataset showed the stability of efficiency and accuracy of the algorithm. The time complexity is low, which is, N is the number objects in the database, k is the cluster number, and t is the iteration time of the algorithm.

VI. CONCLUSIONS AND FUTURE WORK

As the use of mobile ad hoc networks (MANETs) has increased, the security in MANETs has also become more important accordingly. Due to the vulnerability of ad hoc networks, intrusion prevention measures such as encryption and authentication are not enough; therefore, there is a strong need for intrusion detection as a frontline security research area for ad hoc network security.

An intrusion detection system aims to detect attacks on mobile nodes or intrusions into the networks. In this survey paper, we try to inspect the security issues in the mobile ad hoc networks, which may be a main disturbance to the operation of it. We then discussed some typical and dangerous vulnerabilities in the mobile ad hoc networks, most of which are caused by the characteristics of the mobile ad hoc networks such as mobility, constantly changing topology, open media and limited battery power. Then we discussed attacks on Mobile Ad hoc Networks. Finally, we introduce the security schemes in the mobile ad hoc networks that can help to protect the mobile ad hoc networks.

During the survey, we also find some points that can be further explored in the future, such as to find some effective security solutions and protect the MANET from all kinds of security risks. We will try to explore deeper in this research area.

REFERENCES

[1] R. Nakkeeran, T. Aruldoss Albert and R. Ezumalai, “Agent Based Efficient Anomaly Intrusion Detection System in Ad hoc Networks”, IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

[2] R. Saminathan, Dr. K. Selvakumar, “PROFIDES - Profile based Intrusion Detection Approach Using Traffic Behavior over Mobile Ad Hoc Network”, International Journal of Computer Applications (0975 – 8887) Volume 7– No.14, October 2010.

[3] Li Bo and Jiang Dong-Dong, “The Research of Intrusion Detection Model Based on Clustering Analysis”, International Conference on Computer and Communications Security, 2009 IEEE.

[4] Peyman Kabiri and Mehran Aghaei, “Feature Analysis for Intrusion Detection in Mobile Ad-hoc Networks”, International Journal of Network Security, Vol.12, No.2, PP.80–87.

[5] L. Prema Rajeswari, R. Arockia Xavier Annie, A. Kannan ,“Enhanced Intrusion Detection Techniques for Mobile Ad Hoc Networks”, IET-UK International Conference on Information and Communication Technology in Electrical Sciences (ICTES 2007), Dec. 20-22, 2007.

[6] Ali Ghaffari. “Vulnerability and Security of Mobile Ad hoc Networks”, Proceedings of the 6th WSEAS International Conference on Simulation, Modelling and Optimization, Lisbon, Portugal, September 22-24, 2006.

[7] Pin Nie, “Security in Ad hoc Network”,2006.

[8] Xia Wang, Tu-liang Lin, Johnny Wong, “Feature Selection in Intrusion Detection System over Mobile Ad-hoc Network”.

[9] Abhay Kumar Rai, Rajiv Ranjan Tewari & Saurabh Kant Upadhyay, “Different Types of Attacks on Integrated MANET-Internet Communication”, International Journal of Computer Science and Security (IJCSS) Volume (4): Issue (3).

[10] Karan Singh, R. S. Yadav, Ranvijay, ”A Review paper on Ad Hoc Network Security”, International Journal of Computer Science and Security, Volume (1): Issue (1).

[11] Levente Butty, Jean-Pierre Hubaux, “Report on a Working Session on Security in Wireless Ad Hoc Networks”, Mobile Computing and Communications Review, Volume 6, Number 4.

[12] Y. Huang, W. Fan, W. Lee, and P. S. Yu, “Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies”, Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, 2003, pp. 478-487.

[13] Oleg Kachirski, Ratan Guha, “Intrusion Detection Using Mobile Agents in Wireless Ad Hoc Networks”, Proceedings of the IEEE Workshop on Knowledge Media Networking (KMN’02) 0-7695-1778-1/02 $17.00 © 2002 IEEE.

[14] Janne Lundberg, “Routing Security in Ad Hoc Networks”, Tik-110.501 Seminar on Network Security HUT TML 2000.

[15] R. Heady, G. Luger, A. Maccabe and M. Servilla, “The Architecture of a network level intrusion detection system”, Technical Report, Computer Science Department, University of New Mexico (August 1990).

[16] Meng Jianliang Shang Haikun Bian Ling, “The Application on Intrusion Detection Based on K-means Cluster Algorithm”, International Forum on Information Technology and Applications, 2009 IEEE.

Preetee K. Karmore pursuing M. E. 4th Semester in Wireless Communication and Computing from G. H. Raisoni College of engineering, Rashtrasant Tukadoji Maharaj Nagpur University, Nagpur, India.