Volume 3, Issue 11, November 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Testing of Wormhole Detection Mechanism based on Clustering

Jagteg Singh[1],
[1] Research Scholar,
Department of Computer Science,
Global Institute of Management and Emerging Tech.,
Amritsar, India

Er.Prabhdeep Singh[2]
[2]Assistant Professor,
Department of Computer Science,
Global Institute of Management and Emerging Tech.,
Amritsar, India

Abstract— Wireless sensor networks is special type of ad-hoc network in which devices are connected on each and work independently in a collective manner to achieve a combined specified work which will be sent to the sink (base station). Routing in wireless sensor network is usually based on various protocols, some of which are proactive and some of them are on demand nature. Ad-hoc On Demand Distance Vector protocol is a popular and reliable protocol used for global communication in ad-hoc manner and it is widely acceptable and most used protocol in routing of wireless sensor network. Due to limited energy carrying property of the wireless sensor nodes, many attacks always seeks to breach into the network. Especially in case of on demand routing, vulnerabilities increases due to nature of routing. Ad-hoc On Demand Distance Vector Routing protocol is one of the most used and energy saving protocol implemented in sensor network but have low security. Attacks such as wormhole and phising are most occurring attacks in the AODV due to nature of routing. Wormhole is most occurred network attack in AODV. In this paper, we have done analysis of the clustering based approach for detecting the wormhole attack. To accomplish this, a clustering based on K-means has been implemented with time synchronization of the time intervals in between source and destination. The performance of the network has been judged on the bases of Number of Hops, Delay, Traffic Received and Throughput. The simulation is carried in OPNET Modeler 14.5 simulator.

Keywords— Wormhole Attack, Adhoc On Demand distance Vector Protocol, Clustering, On Demand Routing Protocols, Route Request, Route Reply, Mobile Ad-hoc Network, Time Synchronization.

I. INTRODUCTION

In all possible methods of attacks in Mobile Ad hoc Networks (MANETs), the wormhole attack is the most dangerous and sort of hidden attack. Wormhole attack usually has two attacker nodes which create a tunnel by skipping other nodes and start transfer information to other end of attacker node. Malicious nodes have different range and can be placed on different locations which perform a tunnel of high speed link via a secrete channel. [15]

These nodes can act as router or host or both at same time. They can form random topologies depending on their connectivity with each other in the network. [16] These nodes have the ability to arrange themselves and because of their self-configuration ability, they can be deployed immediately without the need of any infrastructure. The major performance constraint comes from path loss and multiple path fading. Many MANET routing protocols exploit multiple paths to route the packets. [17]

II. WORMHOLE ATTACK

Wormhole attack is a dangerous and difficult attack to deal with. A small demonstration of overview for wormhole attack is given in figure 1 below. In any ad-hoc network, a wormhole can be created through the following ways:

- Tunneling of packets above the network layer
- Long-range tunnel using high power transmitters

In the first type of wormhole, all packets which are received by a malicious node are duly modified, encapsulated in a higher layer protocol and dispatched to the colluding node using the services of the network nodes [3]. These encapsulated packets traverse the network in the regular manner until they reach the collaborating node. The recipient malicious node, extracts the original packet, makes the requisite modifications and sends them to the intended destination.

In the second and third type of wormholes, the packets are modified and encapsulated in a similar manner. However, instead of being dispatched through the network nodes, they are sent using a point to-point specialized link between the colluding nodes. In this thesis, we only discuss solutions to the first type of wormhole, which in our opinion has greater applicability to pure ad-hoc networks [5].

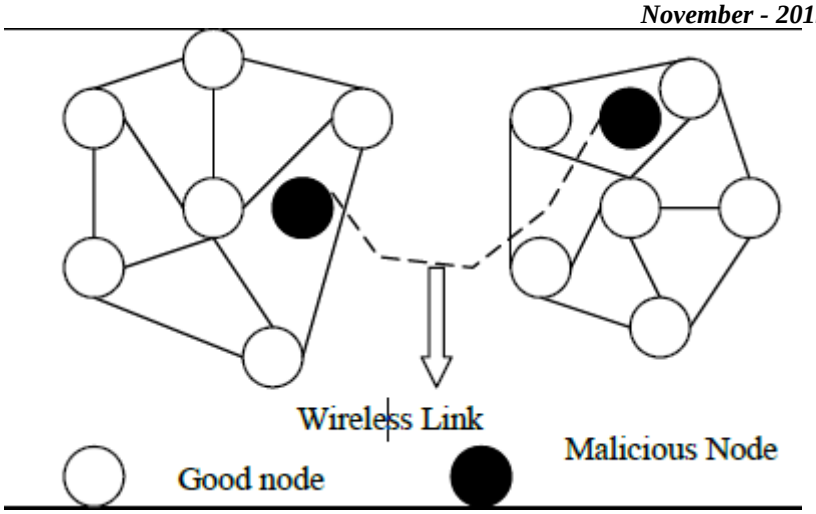

Figure 1: Wormhole attack demonstration

It is very important when considering security issues of network, is wormhole attack, which is difficult to detect & can harm by directing important data to unauthorized nodes. [6] [7] [8] During the route discovery process, a wormhole can relay route request and response messages between distant nodes, creating the appearance of shorter routes to destinations. [9] [10] [11] Since the wormhole can be anywhere along a route, a source will have to detect its existence somewhere along the route when a node sets up the route (on-demand). [12]

.

III. PROPOSED SOLUTION

We have focused on providing solution for said problem by enhancing multipath algorithm resulting in regaining of the average no. of hops as well to get normal delay by excluding the attacker nodes. To avoid the wormhole attack, proposed algorithm will be implemented in scenario affected by wormhole attacks and this will try to normalize the scenario to its original state. The parameters for Random waypoint have been shown in figure 2 below.

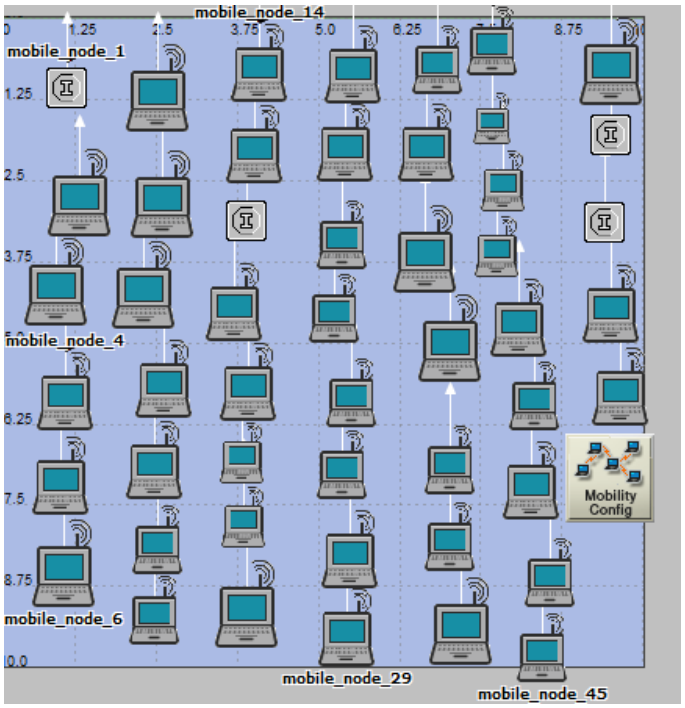

Figure 2: Overall simulation with random waypoint model for mobility

In neighbor discovery each node records the time init T and broadcasts a HELLO message for the neighbor discovery immediately after the deployment of the sensor nodes. Each node that receives a HELLO message sends a reply. Each node builds its neighbor list which could include remote neighbors connected by a wormhole and calculate the time of arrive (ToA) overhead. Packet header will carried the packet forward, packet sent, packet received, time to live and next hop address filed. In case of wormhole detection, drop packet field will increase more than normal count. If it is more than threshold number decided then it is consider being the malicious node. The basic idea behind using the k-means cluster analysis to detect wormhole attack relies on the distance correlation in the physical locations of nodes. According

to the ToA calculate from the legal part and illegal part with different identities overhead time, we can apply the k-means cluster analysis to the mixture of these two ToA streams. Due to the assume analysis, the distance between comprise nodes is long enough. We explore the k-means algorithm, which aims to partition n observations into k clusters. The ToA is chosen as the dissimilarity measure. In our scheme, k is equal to 2. Basic parameters like energy carrying capacity, buffer size, speed of nodes, mobility rate and average error rate for AODV have been used.

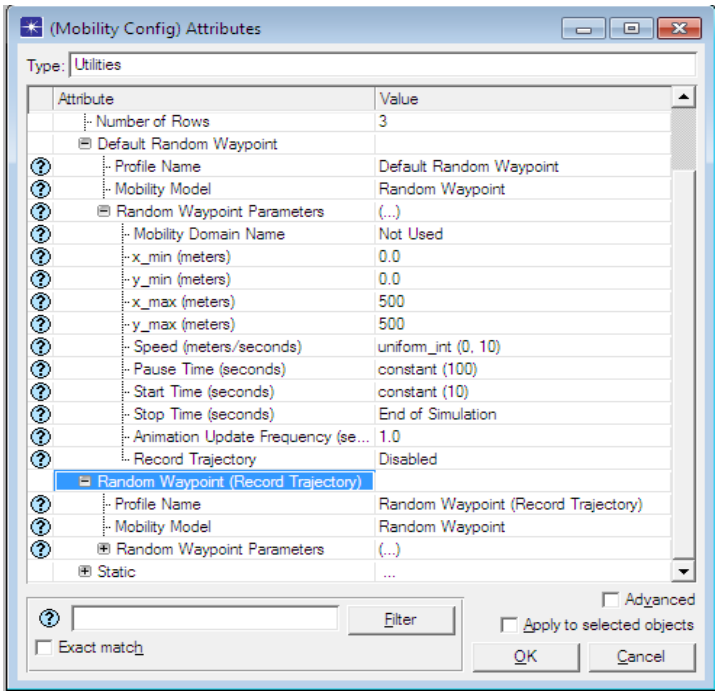

Figure.3: Configuration of Random Waypoint model for mobility

After basic building, implementation of wormhole attacks has been implemented by making an attacker transmitter and attacker receiver. Implementation has shown the wormhole attack effects on normal wireless sensor network. Both scenarios has been compared on the bases of parameters like throughput, number of hops, end to end delay and network load.

To avoid the wormhole attack, proposed algorithm has been developed and implemented in scenario affected by wormhole attacks and this tried to normalize the scenario to its original state. Proposed algorithm, k means cluster have been formed with invoking process of header which is shown in figure 3 For elimination of the wormhole node, architecture based changes has been done for overtaking the effect of wormhole. The node architecture of normal scenario (Figure 4) and node architecture changes (Figure 5) are given below.

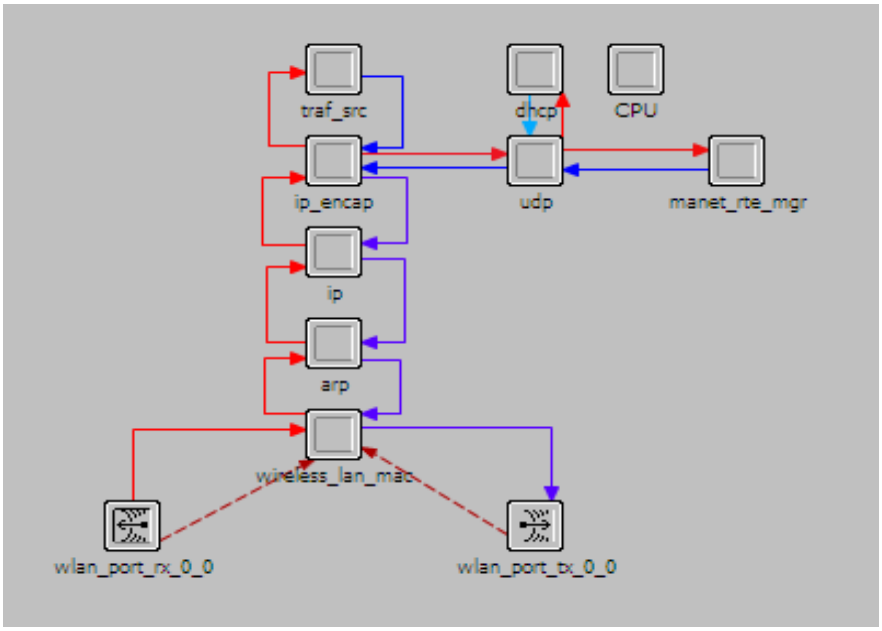

Figure 4: Node Architecture of normal process of AODV

Below is the changes architecture of the AODV process for eliminating the wormhole affected network. This research use logging modules on medium access layer which use to monitor average metric value used by network while communication. It maintains an average value for delay and number of hops. After implementation of this module, it finds the malicious nodes because the metric values of malicious nodes are very less as compare to normal metric value.

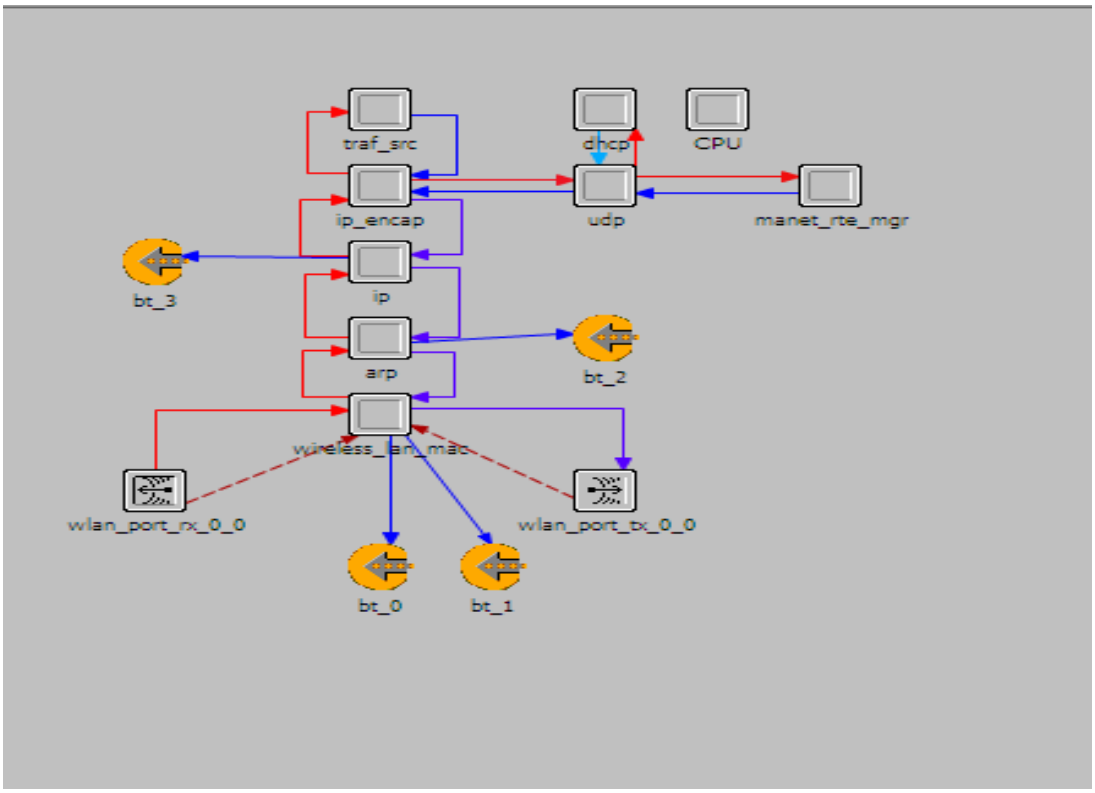

Figure 5: Node Architecture changes done for elimination of Wormhole

Below is header changes architecture of the AODV process for eliminating the blackhole affected network.

```
/* determine the interrupt type */
intrpt_type = op_intrpt_type ();
intrpt_code = op_intrpt_code ();

/* Determine if we are being invoked by one of the child proceses       */
/* maintained by IP. Note that "ip_icmp" is used for ICMP messages      */
/* (currently only supports "ping") and "ip_basetraf_src" is used       */
/* background utilization traffic specification generation.
invoke_prohandle = op_pro_invoker (module_data.ip_root_prohandle, &invoke_mode);
if ((invoke_mode != OPC_PROINV_INDIRECT) && (invoke_mode != OPC_PROINV_DIRECT))
        {
        ip_dispatch_error ("Unable to determine if how IP process got invoked.");
        }
```

Figure 6: Header Architecture changes done for elimination of Wormhole

IV. EXPERIMENTAION

A proposed concept of clustering scheme in which communication is done within clusters and header changes for management of attack scenario is used to avoid the wormhole attack from wireless sensor network.

Table 1: Parameters used for the experimentation

Parameters	Value
Simulator	OPNET
Simulation Time	15 mins
No of nodes	50
Routing Protocol	AODV
Traffic Model	CBR
Pause Time	100 sec
Speed	11 mps
Number of sources	2
Sub-packet size	256 bytes
Transmit Power	15mW
Receiving Power	13 mW
Initial battery power	100j
MAC layer	802.11

For experimentation we have used OPNET 14.5 with animation for the concept of clustering with predicted clustering heads. Various parameters used for experimentation is above table 1:
The detailed experimentation has been consider in the OPNET with clustering approach within sensor area network which will used for solution of wormhole attack with proposed concept. Results obtained for normal performance of AODV, Performance of AODV under wormhole attacks and performance behavior of AODV with elimination of wormhole attacks in term of throughput, delay, number of hops and Traffic Received in AODV network is discussed in the following sections.

PERFORMANCE OF AODV WITH THROUGHPUT OF THREE SCENARIOS

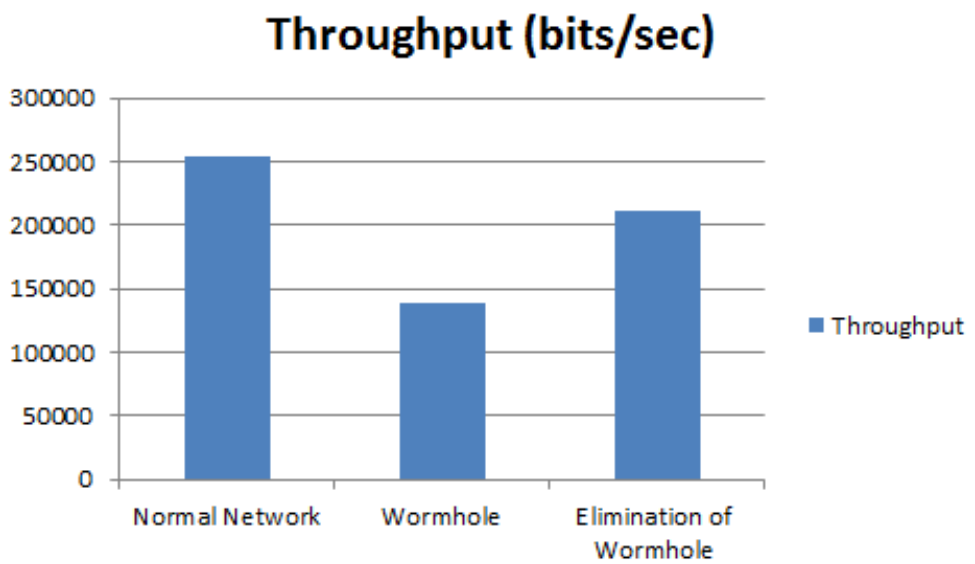

Figure 7: Throughput variation for three scenarios

The performance of network is compared in above figure (Figure 7) and it show that Normal network provide better throughput than network hit by wormhole and network performance tends to decrease when hit with wormhole attack. Recovery mechanism provides good recovery and throughput goes near to normal throughput.

PERFORMANCE OF AODV WITH DELAY OF THREE SCENARIOS

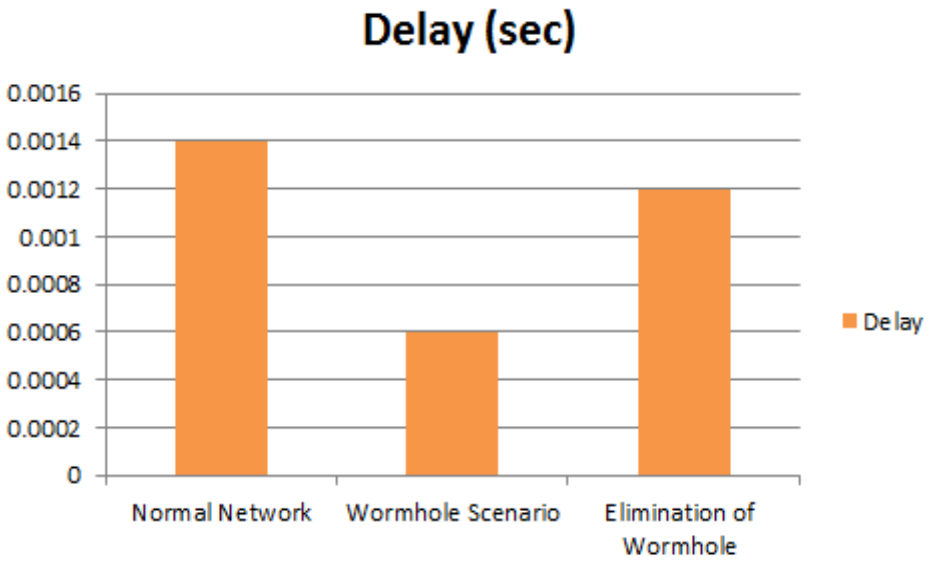

Figure 8: Delay (sec) comparison of all three scenarios

The performance of network is compared in above figure (Figure 8) and it show that Normal network provide better throughput than network hit by wormhole and network performance tends to decrease when hit with wormhole attack. Recovery mechanism provides good recovery and throughput goes near to normal throughput.

ANALYTIC RESULTS

The overall simulation performance is presented in nutshell in the following table, which indicates that the elimination of wormhole attack scenario provides the better results and try to normalize the wormhole effected network to its normal state as close as possible.

Table 2: Detailed Result Summary

Attributes	Simulation Time (sec)	Normal Scenario	Wormhole Scenario	Elimination Scenario
Traffic Received (bits/sec)	900	10580	5665	10235
Throughput (bits/sec)	900	250000	139000	210000
Delay (sec)	900	0.0014	0.0006	0.0012
Number of Hops per route (Average value)	900	4.5	2.5	4.4

V. CONCLUSION

In this work, the performance of the wireless sensor network with Ad-hoc on demand distance vector routing protocol has been summarized. The main focus was to show the performance of sensor network protocol AODV under normal environment, under wormhole attack and performance after elimination of wormhole attack in term of packet delivery ratio and overhead. In doing so, a wormhole scenario has been created and four wormhole attacker nodes have been generated. These malicious nodes provide false information to the network and AODV consider the path defined by malicious nodes as best routing path available and start communication through it. Performance of network decreases after wormhole attack and to eliminate of this attack, K-means clustering approach with header changes have been opted and implemented in network while communication. It maintains an average value for delay and number of hops. After implementation of this module, it finds the malicious nodes because the metric values of malicious nodes are very less as compare to normal metric value. A summary of suspected nodes has been forwarded to the upper layer where another module has been added to find the sequence of attack. If any sequence found, it is sent to network layer where another module is added to find the solution for attacks. Elimination of nodes takes place on Network layer by broadcasting the information of malicious nodes. Overall, elimination of wormhole attack has been done so that wireless sensor network communication can be normalized as normal communication.

REFERENCES

[1] TIAN Bin, LI Qi, YANG Yi-xian, LI Dong, XIN Yang, ''A ranging based scheme for detecting the wormhole attack in wireless sensor networks'', Science Direct, pp. 6-10, Vol. 19, June 2012.

[2] Ali Modirkhazeni, Saeedeh Aghamahmoodi, Arsalan Modirkhazeni, Naghmeh Niknejad," Distributed Approach to Mitigate Wormhole Attack in Wireless Sensor Networks", Wireless Engineering and Technology, IEEE, pp. 142-151, Vol. 3, 2012.

[3] Thanos Stathopoulos, Rahul Kapur, Deborah Estrin, "Application-Based Collision Avoidance in Wireless Sensor Networks", Conference of Computer society, pp. 335-343, July-December 2005.

[4] Kuldeep Kaur, Vinod Kumar & Upinderpal Singh, "Detection of Wormhole Attack in Wireless Sensor Networks," IRNet Transactions on Computer Science and Engineering, 2011.

[5] Guiyi Wei Xueli Wang "Detecting Wormhole Attacks Using Probabilistic Routing and Redundancy Transmission". WASE International Conference on Information Engineering, pp. 251-254, 2010.

[6] Dhara Buch and Devesh linwala, "Detection Of Wormhole Attacks In Wireless Sensor Network", Proc. of Int. Con! on Advances in Recent Technologies in Communication and Computing, IEEE, 2011.

[7] Lukman Sharif and Munir Ahmed," The Wormhole Routing Attack in Wireless Sensor Networks (WSN)", Journal of Information Processing Systems, pp. 345-347, Vol.6, Issue.2, June 2010.

[8] Dhara Buch and Devesh Jinwala" Prevention of Wormhole Attack In Wireless Sensor Network ", International Journal of Network Security & Its Applications (IJNSA), Vol.3, Issue.5, Sep 2011.

[9] Dezun Dong, Mo Li, Yunhao Liu And Xiangke Liao, "Connectivity-Based Wormhole Detection in Ubiquitous Sensor Networks", Journal Of Information Science And Engineering Vol.27, pp. 65-78, 2011.

[10] Sebastian Tere," Secure Route Discovery against Wormhole Attacks in Sensor Networks using Mobile Agents", IEEE, Vol.11, 2011.

[11] Ms. N.S.Raote, Mr.K.N.Hande, "Approaches towards Mitigating Wormhole Attack in Wireless Ad-hoc Network", International Journal Of Advanced Engineering Sciences And Technologies, Vol.2, No. 2, pp 172 – 175, June 2010.

[12] Dr. Karim Konate, Abdourahime Gaye, "A Proposal Mechanism Against the Attacks: Cooperative Blackhole, Blackmail, Overflow and Selfish in Routing Protocol of Mobile Ad Hoc Network", International Journal of Future Generation Communication and Networking, Vol. 4, No. 2, pp 156-158, June 2011.

[13] Reshmi Maulik, Nabendu Chaki, "A Study on Wormhole Attacks in MANET", International Journal of Computer Information Systems and Industrial Management Applications, Vol. 3, No. 1, pp 271-279, January 2011.

[14] Gajendra Singh Chandel, Priyanka Mur, "Manet Threat Alarming Based On System Statistics & Support Vector Machine", International Journal of Engineering Research and Applications, Vol.2, No. 4, pp 1722-1726, August 2012.

[15] A.Shevtekar, K.Anantharam, N.Ansari, "Low Rate TCP Denial-of-Service Attack Detection at Edge Routers," IEEE Communication Letters, Vol.9, No. 4, pp 363–65, April 2005.

[16] Amol A. Bhosle, Tushar P. Thosar, SnehalMehatre, "Black-Hole and Wormhole Attack in Routing Protocol AODV in MANET", International Journal of Computer Science, Engineering and Applications , Vol.2 , No. 1, pp 325-331, February 2012.

