A HYBRID OUTLIER DETECTION APPROACH WITH MULTI DIMENSIONAL FEATURES TO PREVENT BLACK HOLE ATTACK IN MANET

[1]**Ibrahim Salim.M**

Research Scholar, Research and Development Centre, Bharathiar University, Coimbatore, Tamil Nadu and Assistant Professor, Department of Computer Applications,
MES College Marampally, Aluva, Kerala, India.
mes.ibrahimsalim@gmail.com

[2]**Dr. T Abdul Razak**

Associate Professor,Department of Computer Science,
Jamal Muhammed, College, Thiruchirappally,
Tamil Nadu , India
abdul1964@yahoo.com

[3]**Dr. Murugan R.**

Associate Professor and Head
Department of Computer Applications
MES College Marampally, Aluva, Kerala , India
mes.murugan@gmail.com

Abstract

An increase in the technological upgrades in the mobile communication technology has led to the tremendous increase in the usage of mobile networks. Mobile Adhoc Network is an instantaneous network where the requirement of the infrastructure is not mandatory. This feature has raised a lot of issues in the security aspects of the MANET. The mobility of the nodes, frequent topological changes, weak communication link and lack of infrastructure are the critical factors creating security issues in MANET. The security issues leads to lot of routing attacks, which disturbs the network communication and completely collapse the system. One such attack is the black hole attack. The AODV routing protocol is more vulnerable to the black hole attack. This paper proposes an efficient approach based on outlier detection techniques to detect and prevent the black hole attack in MANET. The results have been simulated using the NS2 simulator and performance of the algorithm has been evaluated based on various performance metrics like packet delivery ratio, routing overhead, detection efficiency ratio and end to end delay time .

Keywords: MANET, Security Issues, Black Hole Attack, AODV, Performance metrics**.**

1.Introduction

MANET is becoming very popular because of the huge variety of networking Competence for the cellular device customers. There are enormous applications offered by MANET in the real world scenario. But the dynamic topological feature of the MANET does not assure the guarantee for the secured data transmission. MANET is liable to different types of attacks. Any type of routing attack in MANET will disturb the whole communication and the complete network may be distorted. Black hole attack is one such attack which degrades the performance of the routing protocol in the MANET.

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

The Black Hole attack [11] is an attack where an abnormal node broadcasts itself as it has the shortest optimal route to the destination and forwards the duplicate RREP packet to the source node. The source node establishes the route through the abnormal node and starts the data packets to flow through the abnormal node. The abnormal black hole nodes drop all the packets within itself, thereby disabling the source and destination node's communication. AODV routing protocol[10] is vastly affected by the black hole attacks. The black hole Node terribly decreases the packet delivery ratio through no longer forwarding the data packets to the destination. The malicious Black hole node primarily affects the control packets like RREQ, RREP and RERR. Spoofing the control packets will be more advantageous for the black hole node. The malicious node drop the RREQ packets to prevent the route establishment through it and saves its energy for transmitting its own packet. Black hole node may also try to drop the RREP packet which results in high delay in the route discovery process, thereby initiating the new route discovery process. The repeated initiation of new route discovery process will escalate the routing overhead of the protocol. RERR packets are dropped to extend the usage of the damaged routes so that source node keeps communicating the packets through the broken route. The black hole node drops all the data packets towards it. [12].The Network throughput declines subsequently as the black hole node drops all the data packets with in itself. Many black hole detection and prevention techniques are available to detect and prevent the black hole attacks in MANET.

2. Related Work

C.W. Yu et al [1] proposed a distributed cooperative mechanism (DCM) to avoid black hole attacks, by checking data packets transmitted by neighboring nodes. If a node has not transmitted any data packets within a fixed time-threshold, then the checking node will transmit a "test packet", intended for another cooperating detection node through the suspicious node. If the destination receives the "test packet," then the suspicious node is legitimate; otherwise, it is considered malicious. The drawback of this scheme is that malicious nodes may try to exploit this mechanism, by analyzing the duration of time before a malicious node is detected and subsequently, the routing of at least one packet within this time-frame.

Latha Tamil Selvan et al [16] proposed a mechanism to detect black hole attacks by checking if the SQN of a RREP message is higher than a dynamic threshold value, which is an indication of a blackhole attack. The value of the threshold is updated by calculating the difference between the SQNs of the RREP message and the average of the previously received SQNs. Moreover, the proposed solution requires many significant modifications to the AODV protocol.

A detection mechanism called the Anti-Black hole Mechanism was proposed by Ming-Yang Su[4], which captures both RREQ and their consistent RREP messages and estimates the difference between the two. When this difference exceeds a predefined threshold, an alarm is raised informing all nodes on the network to cooperatively isolate the malicious node. This mechanism requires each node to run in promiscuous mode in order to capture, store, and process the RREQ and RREP messages within their radio range. Therefore monitoring nodes are hindered with computational and storage overheads, as well as increased energy consumption.

MenakaPushpa[2] proposed a modified approach of AODV which is based on trust and gives equal weight to both route trust and node trust for the route selection process. Continuous evaluation of node's performance and collection of neighbor node's opinion value about the node are used to calculate the trust relationship of this node with other nodes.

Medadian et al. [4] present a routing protocol to combat black hole attack in MANET. It is a trust based method where the sender takes opinion of the neighbors of the node (say, node A) which replied with a RREP packet, i.e., advertises the shortest route to the destination. This opinion along with a rule base determines whether node A is malicious.

Satoshi Kurosawa [8] presented a new detection method based on dynamically updated training data. Through the simulation, our method shows significant effectiveness in detecting the black hole attack. C. Panos[5] proposed a methodology named a

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

specification-based intrusion detection engine for infrastructure-less networks.

There are wide varieties of detection and prevention mechanism [9],[14],[15] available to detect black hole attack in MANET.

3. Problem Statement

Security in MANET is an important issue during data transmission. Routing misbehavior of the black hole nodes can sternly damage the performance of the routing layer. The Black hole nodes can participate in the route discovery and maintenance and data transmission phase. They deny forwarding the data packets. Some black hole nodes can be detected during the route discovery phase, when the nodes refuse to forward the RREQ packet. Some nodes tend to be legitimate during the route discovery phase and exhibit their misbehavior during the route maintenance and data transmission phase thereby refusing to forward the data packets and RRERR packets. This paper focus on detecting the black hole node and improve the performance of routing protocol with low routing overhead and improved packet delivery ratio.

4. Proposed System

To detect the black hole node in the MANET during route discovery process, the delay time in transmitting the RREP to the source node(S) is considered. If the source node wants to send a data to the destination node, it checks its route look up table, to check the availability of the route to the destination node (D). If any data transmission has taken place , The route look up table will get updated with the route to the destination node .If there is no routing information available, then source node (S) will broadcast the RREQ packet to the neighboring nodes. The neighboring nodes which receive the RREQ packet will check whether the packet is designated to it, otherwise the RREQ packet is again broadcasted to its intermediate neigbours. This process continues until the destination node (D) receives RREQ packet. The RREP packet will be unicasted by the destination node in the route it received the RREQ Packet. Once if the source node receives the RREP, it checks whether the RREP has been received with in the estimated delay time. If it receives the packet after the estimated delay time then the route with the shortest communication cost is established and the data transmission takes place. This scenario takes place when all nodes are considered as the normal node.

Case 1: All nodes are legitimate nodes. $\{x_{\alpha\beta}\}$ where $\alpha\beta$ ={S1,A2, B3,C4,D5},where β={ 1 *to* n} where each $x_{\alpha\beta} \geq$ DT $_{Ths.}$.Where α be the set of nodes and β be the associated delay time of the respective nodes. Let us assume that α={S,A, B,C,D} are all legitimate nodes and its delay time is$\geq$ DT $_{Ths}$.The following figure4.1 illustrates Case1.

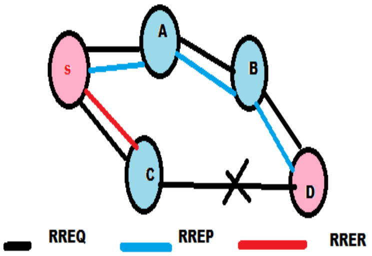

Figure4.1: Scenario with all nodes as Legitimate nodes

Node S broadcast the RREQ to A and C. A and C checks the address and further broadcast the packet. A sends to B and C sends to D. As the link between C to D has failed C forwards RERR message to S. B in turn forwards the Packet to D. D replies S by unicasting the RREP through D-B-A-S. S checks whether the delay time of the RREP received from A is $\geq$ DT $_{Ths}$establish the route and starts transmitting the data packet. Suppose if any of the intermediate node tends to misbehave like the black hole node, then that node will immediately reply back to the source node, without checking the route look up table. The RREP packet from the black hole node will reach the source node (S) before the delay time. The source node considers such nodes as the black hole node and broadcast the same to the neighboring nodes to ignore any communication via the black hole node.

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

4.1 Analysis of Black Hole Node

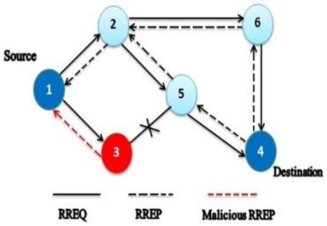

Figure 4. 2: MANET scenario with Malicious nodes

Case 2: All nodes are not legitimate nodes.{$x_{\alpha\beta}$} where α={1 to n} and β={ 1 *to*n} where each $x_{\alpha\beta} \geq$ DT $_{\mathit{Ths.}}$ .Where α be the set of nodes andβ be the associated delay time of the respective nodes. Let us assume that α={1,2,4,5,6} are all legitimate nodes and its delay time is≥ DT $_{\mathit{Ths}}$.Figure 4.2 illustrate the case 2 that all nodes are note legitimate.Node 3 is a black hole node. It will not forward the RREQ to node 5. It will immediately reply to the source node 1 with the RREP with the delay time ≤DT $_{\mathit{Ths.}}$ *Now the source node checks the delay time and concludes that Node 3 is malicious node and broadcast the information to all other nodes in the network.*

The Dynamic topological nature of the MANET may lead to lot of inconsistency, while considering the delay time as a parameter to identify the black hole node. Any node may enter into the network or leave the network at any point of time. This leads to a variation in the calculated delay time and Hopcount in the Network. In such cases, there are chances to wrongly assume the malicious node as a legitimate node.

Case3:Let C be the cluster of nodes {A…Z} Where X is a subset {$x_{\alpha\beta}$} where $\alpha_1\beta_1$={S1,A2, B3,C4,D5},where β_1={ 1 ,2,3,…,n} where each $x_{\alpha\beta} \geq$ DT $_{\mathit{Ths.}}$ *Let* Y={E,F,…Z} where $\alpha_2\beta_2$={ E1,F2,…Zn} where β_2={ 1 ,2,3,…,n}and Let Z={ C,E,…,Z}where $\alpha_3\beta_3$={ C1,E2,…Zn} where β_3={ 1 ,2,3,…,n} . Due to Dynamic topological nature, nodes present in the subset

X may change as X={{$x_{\alpha1\beta1}$}∪$Y_{\alpha2\ \beta2}$} or X={{$x_{\alpha\beta}$}-Z $_{\alpha3\beta3}$} and viceversa .In such cases, estimated delaytime of the RREP Stored in the Route look up table of source node may vary from the actual delay time of RREP. This may lead to the scenario to assume malicious node as the legitimate node and legitimate node as the malicious node.

In order to avoid this kind of issues, multidimensional feature vector is established. Each dimension is counted upon every time slot. The destination sequence number is taken into account to detect the black hole node.In normal state, each node's sequence number changesdepending on its traffic conditions. However, when the number of nodes in the network increases the destination sequence number also increases. However, when the black hole attack take place, the sequence numberis increased largely. When the destination sequence number given by the black hole node is less than the maximum sequence number of the network, then it leads to a dilemma to consider the destination sequence number in the RREP packet recieved from the malicious node is a valid sequence number. In such case, the black hole node is tend to be treated as a normal node.

Type[8]	Reserved[16]	Hop Count[8]
RREQ ID [32]		
Destination IP Address 1[32]		
Destination IP Address 2[32]		
Destination Sequence Number[32]		
Source IP Address[32]		
Source Sequence Number[32]		

Figure 4.3 : RREQ Packet Format

The Figure 4.3 and Figure 4.4 represents the RREQ and RREP Packet format . The size of the field is represented in terms of number of bits.

Type[8]	Pfx Length[8]	Hop Count[8]
Destination IP Address 1[32]		
Destination Sequence Number [32]		
Source IP Address[32]		
IP Address of node that first generate RREP [32]		
Life Time [32]		
Destination Sequence Number [32]		

Figure 4.4 : Route Reply Packet Format

With these features , the average difference of destination sequence number in each time slot between the sequence number of RREP message is calculated.When a RREQ message is forwarded , each

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

node records the destination IP address and the DstSeqNo in its list. When a RREP message is received, the node looks over the list to see if there is a same destination IP address. If it same , the difference of destination sequence number is calculated, and this operation is executed forevery received RREP message.Therefore average difference on sequence number is selected as a feature.

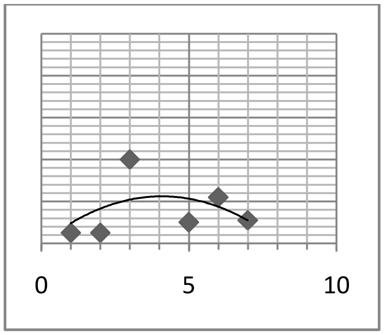

Figure 4.5 : Outlier model of Black Hole node Detection

For the communication flow by the node , the node's istance state in the network in time slot iis expressed by three-dimension vectorsxi= (sxi1, sxi2, sxi3). Here, the nodes in the normal state is gathered in the group and nodes that deviate and scatter from the cluster of the normal node is considered to be the black hole node. The Figure 4.5 illustrates the outlier model of the Black hole node detection.

Mean vector sxiD using training data set D of N time slots is calculated as follows

$$\overline{sxi}D = \frac{1}{N}\sum_{i=1}^{N} sxi \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(1)$$

Next, distance from input data sample $sx_i$to the mean vector sx_i¯D is calculated as follows

$$d(sx) = ||sx\text{- } xi\text{¯}D||2 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2)$$

Ifd(sx)>Then it will be considered as an black hole attack. If d(sx) <=Th, then the nodes are considerd to be in the normal range.The threshold range is calculated using the following equation.

$$T_h = d(sx_i), \text{ where } I = arg_i max_{xi \in D} d(xi) \ldots\ldots..(3)$$

Let T_0 be the first time interval for a node participating in MANET. By using data collected in this time interval, the initial mean vector is calculated, then the calculated mean vector will be used to detect the attack in the next period time interval ΔT .If the state in ΔT is judged as normal, then the corresponding data set will be used as learning data set. Otherwise, it will be treated as data including attack and it will be consequently discarded. By repeating this process , the Black hole nodes are detected effectively.Other than the Average node distance in the network , the features like number of RREQ and RREP packets successfully forwarded by the nodes are considered.Along with RREQ and RREP, Every node maintains the Reliability Factor (RF) value for its neighbor nodes. Reliability Factor is a counter value where its value will be increased when a node forwards a RREQ and RREP packets. When a node receives the RREP , it checks the reliability factor value , if the value is more than the threshold value ,then it forwards the RREP to the next node. Otherwise it simply discards the RREP packet and declare its sender as a black hole node . Same procedure is applied for RREQ packet also to prevent the black hole node.

5. Performance Analysis

To analyze the performance, of Hybrid Multi-Dimensional Approach(HDMA), the methodology is executed in the scenario with the existence of the black hole nodes. The metrics like Detection efficiency ratio and packet delivery ratio, End to end delay time and Routing overhead are used for analyzing the results.

Metrics	HMDA	**DLM**
Misbehaving Detection Efficiency (%)	40.2 – 90.3	20.2 -80.3
Packet Delivery Ratio (%)	93.9 - 89.6	89.8-85.2
End to end delay (msec)	10.2-27.8	4.8-19.2
Overhead (pkts)	0.0017-0.0041	0.0014-0.0037

Table5. 1: Performance Analysis of the Hybrid Multi-Dimensional Approach

The performance of the methodology is analyzed by varying the number of black hole nodes initiating packet dropping attacks from 20 -100. Based on the traffic involving in a destination node, its Destination sequence number may vary. In the blackhole attack, the consequence of the attack may also change depending on the increased amount of Destination sequence number . Here, we specifically investigate the effects of the attack when the number of Connections to the destination and the number of connection from the destination are changed. Table 5.1 illustrates the performance of HDMA with respect to the above mentioned metrics when compared with the Dynamic learning methodology proposed by Satoshi Kurosawa [8].

Figure 5.1 shows the results of misbehavior detection efficiency by varying the mobility of the nodes from 20 to 100 nodes. From the results, it is observed that HDMA scheme has higher detection efficiency than DLM. HDMA has the higher detection efficiency in the range of 90.31 to 40.2%. The detection efficiency ratio of DLM is in the range of 80.3 to 20.2%.

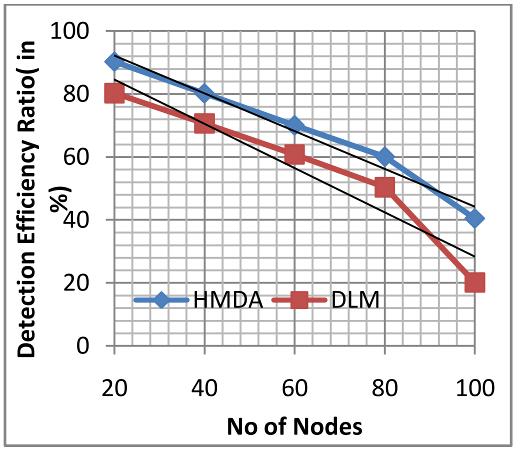

Figure 5.1: Analysis of Detection Efficiency Ratio

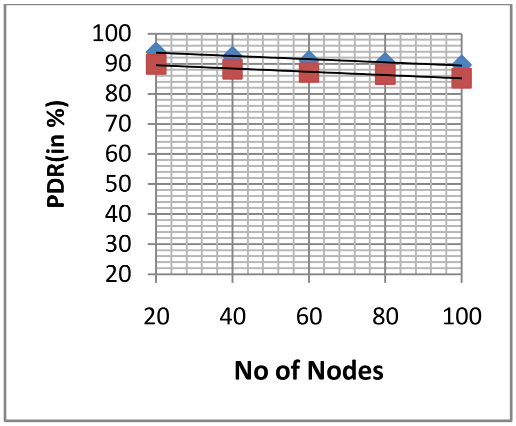

Figure 5.2: Analysis of Packet Delivery Ratio

The Figure 5.2 shows the results of packet delivery ratio by varying the mobility of the nodes from 20 to 100 nodes. HDMA scheme has achieved high packet delivery ratio than DLM scheme. HDMA has the high packet delivery ratio in the range of 93.9 to 89.6%. DLM has the packet delivery ratio in the range of 89.8 to 85.2%.

Figure 5.3 illustrates the performance of the HMDA protocol scheme based on end to end delay time by varying the mobility of the nodes. DLM has the lowest delay time in the range of 4.928-19.327 *msec*. HDMA has the delay time in the range of 10.2 - 27. 8 .The End to End delay time is increased as it checks the multiple dimensions inorder to avoid the black hole nodes.

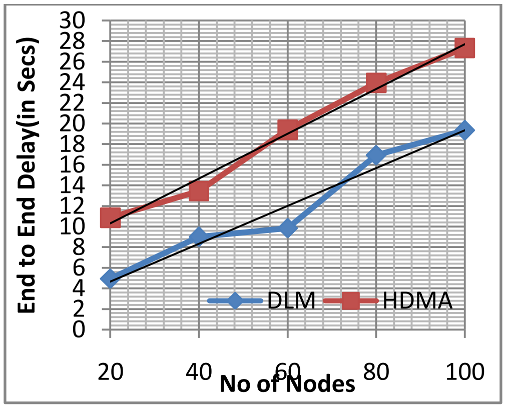

Figure 5.3 : : Analysis of End to End Delay

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

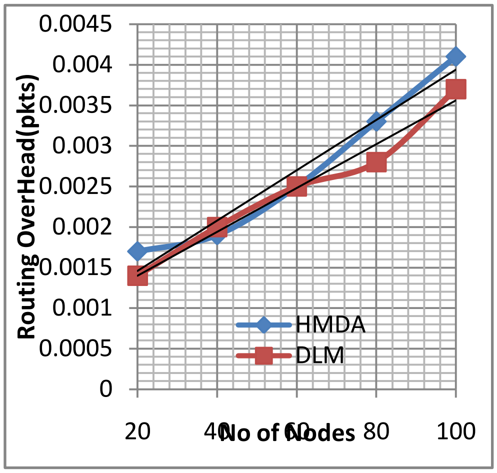

Figure 5.4: Analysis of Routing Overheads

Figure5.4 illustrates the evaluation of routing overhead of the proposed scheme HMDA by varying the mobility of the nodes. DLM has the lowest overhead in the range of 0.0014 *(pkts)* at the mobility rate of 20 nodes and 0.0037*(pkts)* at the mobility rate of 100 nodes. SAOMDV has the overhead in the range of 0.0020-0.00512*(pkts)*. HMDA has the over head ratio in the range of 0.0017-0.0041 *(pkts)* .The proposed scheme has higher routing overhead as the number of features from the route look up table increases.

6. Conclusion

Blackhole attack is one of the most important security problems in MANET. It is an attack that a malicious node impersonates a destination node by sending forged RREP to a source node that initiates route discovery, and consequently deprives data traffic from the source node. This paper, analyses the blackhole attack and introduce s the multidimensional features in order to define the normal state of the network.This proposed solution guarantees the better packet delivery ratio and it is efficient in detecting the misbehaviour nodes when compared with other schemes. The end to end delay time and Routing overhead is comparatively more than the other schemes. In future the proposed scheme will be extended to improve its performance in delay time and routing overheads.

References

[1].C.W. Yu, T.K. Wu, R. H., Cheng, and S. C. Chang, "A Distributed and Cooperative Black Hole Node Detection and Elimination Mechanism for Ad Hoc Networks", PAKDD 2007 Workshops, pp. 538–549, 2007.

[2].A. MenakaPushpa, Trust based secure routing in AODV routing protocol. In: Proceedings of 2009 International Conference on Internet Multimedia Services Architecture and Applications (IMSAA), pp. 1–6. IEEE Press, USA (2009)

[3].Ming-Yang Su, "Prevention of selective blackhole attacks on mobile ad hoc networks through intrusion detection systems", Computer Communications, vol. 34, pp. 107-117, January 2011.

[4].M. Medadian, M. H. Yektaie, A. M. Rahmani, "Combat with Black Hole Attack in AODV Routing Protocol in MANET", AH-ICI 2009, First Asian Himalayas International Conference on Internet, November 2009, pp. 1-5.

[5].C. Panos, C. Xenakis, P. Kotzias and I. Stavrakakis, "A specification-based intrusion detection engine for infrastructure-less networks," Computer mmunications, 54, 67-83, 2014

[6]. Raj PN, Swadas B. (2009). "DPRAODV: A Dynamic Learning System Against Blackhole Attack in AODV based MANET." *International Journal of Computer Science*, Vol 2, PP 54–59

[7]. Su M-Y. (2010). "Prevention of Selective Black Hole Attacks on Mobile Ad Hoc Networks Through Intrusion Detection Systems."*IEEE Computer Communications*, Vol 34, No 1. PP 107–117.

[8]. Kurosawa, S., Nakayama, H., Kato, N., Jamalipour, A., Nemoto, Y.: Detecting Blackhole Attack on AODV-based Mobile Ad Hoc Networks by Dynamic Learning Method. International Journal of Network Security 5(3), 338–346 (2007)

[9]. Jing Xi, Luis Girons Quesada and Yuming Jiang (2007).A Threshold based Hybrid Routing Protocol for MANET. Published in ISWCS 2007, 4th International Symposium Publisher:IEEE, 622 - 626.

[10] K. Sanzgiri, D. LaFlamme, B. Dahill, B. N. Levine,C. Shields, and E. M. B. Royer, "Authenticated routing for ad hoc networks," IEEE Journal on Selected Areas in Communications, vol. 23, no. 3, pp. 598-610, Mar. 2005

[11]. Djenouri D, Badache N. (2008). "Struggling Against Selfishness and Black Hole Attacks in MANETs." *Wireless Communications&MobileComputing. Vol* 8, NO 6, pp 89–704

[12]. Mistry N, Jinwala DC, IAENG, Zaveri M. (2010). "Improving AODV Protocol Against Blackhole Attacks."

SSN (Print): 2204-0595
ISSN (Online): 2203-1731

In Proceedings of the International MultiConference of Engineers and Computer Scientists, Hong Kong.

[13]. Darra E, Ntantogian C, Xenakis C, Katsikas S. A mobility and energy-aware hierarchical intrusion detection system for mobile ad hoc networks. In Trust, Privacy and Security in Digital Business. Springer: Berlin/Heidelberg, 2011; 138–149.

[14]. Ganapathy S, Jaisankar N, Yogesh P, Kannan A. An intelligent system for intrusion detection using outlier detection. In Proceedings of IEEE International Conference on Recent Trends in Information Technology (ICRTIT), Chennai, Tamil Nadu, India, June2011 119–123.

[15]. Y. A. Huang, W. Fan, W. Lee, and P. S. Yu, "Crossfeature analysis for detecting ad-hoc routing anomalies," in The 23rd International Conference on Distributed Computing Systems (ICDCS'03), pp. 478-487, May 2003.

[16].Tamilselvan L,Sankaranarayanan V (2007).Prevention of Blackhole Attack in MANET, the 2nd International Conference on Wireless Broadband and Ultra WidebandCommunications, Sydney, Australia, 27-30.

SSN (Print): 2204-0595
ISSN (Online): 2203-1731