ISSN (Online) : 2277-5420 www.IJCSN.org
Impact Factor: 1.02

A Novel Intrusion Detection System for Detecting Black Hole Attacks in Wireless Sensor Network using AODV Protocol

[1] Umashankar Ghugar, [2] Jayaram Pradhan, [3] Monalisa Biswal

[1,2] Dept. of Computer Science, Berhampur University-760007(India)

[3] Department of Electrical Engineering, NIT Raipur

Abstract - Wireless Sensor Networks (WSN) has wide application in data gathering and data transmission as per the user's requirement and it consist of number of nodes. These nodes have limited battery power, limited resources and limited computational power .Due to all these factors, WSN faces more security threats. Security issues are a vital problem to be solved in Wireless Sensor networks (WSNs). Different types of intrusion detection systems (IDS) are developed to make WSN more secure. In this paper the proposed IDS are based on watchdog monitoring technique and are able to detect Black Hole attacks using AODV (Ad-Hoc On-Demand Distance Vector) Protocol. Besides, the betterment that makes watchdog monitoring technique more reliable are described and the results of simulations of the IDS on NS-2 simulator are presented.

Keywords - *AODV, RREQ, RREP, IDS, PDR, DSR.*

1. Introduction

Wireless sensor network (WSN) is a distributive, autonomous network which consists of nodes (sensor nodes) arranged in a particular environment. These sensor nodes monitor the physical or environmental conditions, such as temperature, sound, vibration, pressure, motion or pollutants, at different areas [1]. A sensor node is a small and simple device with limited computational resources. They are haphazardly and slowly arranged in a sensed environment [2]. Wireless sensor networks are widely used in different applications such as, area monitoring, forest fire monitoring, military surveillance, health care and water quality management. There are number of security issues in WSN. There are some limitations in WSN such as limited lifetime, required low power consumption and less storage [3] [4]. Based on these limitations and because of the rowdy climate in which they are arranged, WSN is very affected and vulnerable to many types of attacks [5].

An intrusion detection system (IDS) is a system which monitors the system or network activities against some malicious activities and informs the main station. The system is generally divided into two categories: misuse IDS and anomaly IDS. In misuse IDS, the malicious activity is evaluated from comparing the new data with the previously stored signature in the database of the system. The abnormal activities in the anomaly IDS is detected from the predefined normal profile [5].Several schemes have been proposed for intrusion detection in WSN. In [6], malicious node is detected by using signal strength in which if the strength is conflict with the originator's geographical position then the message transmission is considered suspicious .Rule-based intrusion detection schemes is used in [7][8]. In rule based scheme, intrusion is detected by a set of rules which are defined before detection phase. These rules are applied on the data obtained from the network behavior. If the data satisfies the rule it is considered normal, else it is considered malicious. An alarm is raised when intruder is detected. Various multipath routing techniques have also been proposed in routing. The objective of this technique is to provide best redundancy path with high energy efficiency [9].

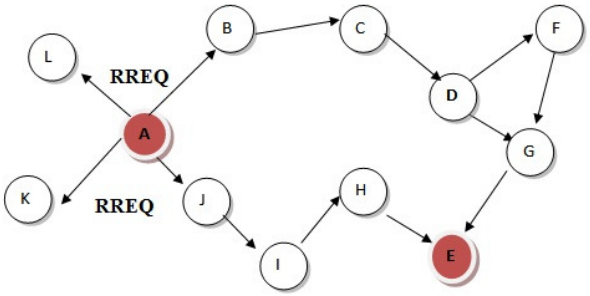
2. Basic Concepts

Black hole Attack:

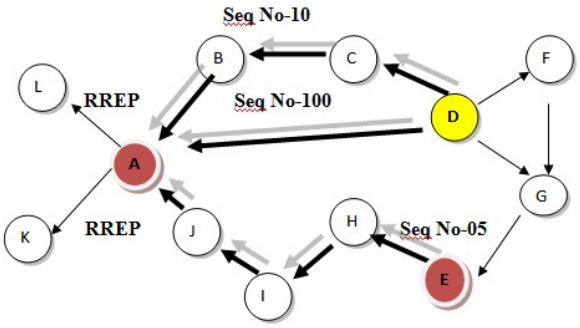
In black hole attack, a malicious node announces itself as the shortest path and attracts all the data traffic towards itself. It consumes all packets without transmitting them to the destination node. The source node starts the route discovery process by broadcasting Route Request (RREQ) packet to its neighbor. The entire neighbor who receives the RREQ forwards it further towards the destination by

adding their address with it. The adversary node sends fictitious Route Reply (RREP) packet (with highest sequence number and least hop count) as a response to source node so as to pretend as a destination node. When the source node receives more than one response; it compares the sequence number of the RREPs received. It selects the path which has the largest sequence number. If both the RREPs have the same sequence number then least hop count is taken in consideration. As RREP from the adversary node has the largest sequence source node sends all data packets to that node. Hence, source node and destination node can neither broadcast with each other [16].

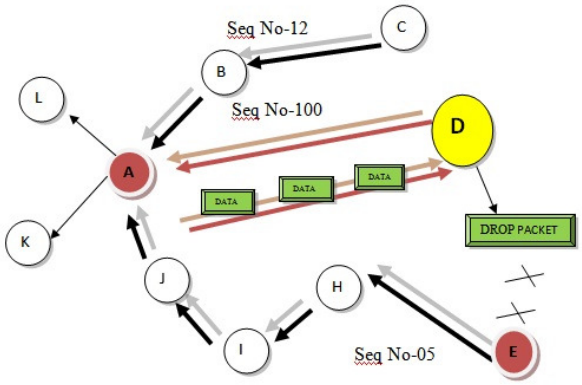
Let's consider the concept in the following figures [18][22].



(a) RREQ broadcast by A



(b) RREP broadcast by Node C, D and E.



(c) Packet Transmit from A to D.

Figure-1

In figure 1(a), the Node 'A' is the Source Node and 'E' is the Destination Node. When 'A' sends the data packets to 'E', it begins the route discovery process by broadcasting Route Request (RREQ) messages to the neighboring nodes [22]. So that the other nodes L, K, B, J in the above figure receive this message.

In figure 1(b), assumed that Node 'D' is a malicious node. It directly sends out fake Route Reply (RREP) message to Node 'A' with highest sequence number as well as the Node 'C' and 'E' also sends a actual Route Reply (RREP) message to Source Node 'A' with sequence number.

In figure 1(c), as per assumption Node 'D' is malicious node but Node 'A' assumes that it is the fresh route and discarded the other entire Route Reply (RREPs) message then it sends data packets to the Destination node. However the Node 'D' drops the entire data packet in place of sending to proper destination. This describe in the figure 1(c).

This is the entire Black hole attack scenario as explain above in Figure 1(a), (b) and (c)

AODV Routing Protocol:

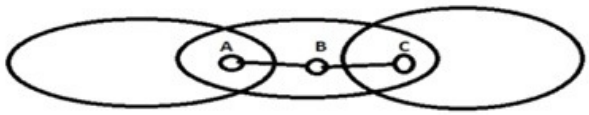
The AODV (Ad-Hoc On-Demand Distance Vector) is frequently used protocol in Wireless Sensor Network. It is also known as dynamic reactive routing protocol [10][17], that automatically route is created on demand basis. When a node sends a data packet to another node, it uses its Routing Table. If it get fresh route then send data packet from source to destination. If it does not get the fresh route then the node starts the Route Discovery Process. In AODV route discovery process has two control messages i.e. Route Request (RREQ) and Route Reply (RREP). To deter mine the fresh route both control messages are used.

After completing the route discovery process, the source node and destination node can be communicate the data packets between them.

Watchdog Technique:

Watchdog technique [19, 20] is the method how to detect misbehaving nodes. It is based on the concept of the broadcast communication in sensor networks, where each node can hear the communication of neighboring nodes even if it is not intended. This technique is depends on the fact that sensors are generally slowly arranged. In this technique each packet transmitted in the network is monitored by neighboring nodes which are in the radio range of sender. They watch the behavior of the node to see whether it forwards correctly the packets it receives. That is watchdog approach [15].

Suppose that a packet should follow the path A→B→C. Node A can inform if node B forwards the packet to node C, by listening promiscuously to node B's transmission. By promiscuously we mean that since node A is within range of node B, it can overhear communications to and from B.



In this Figure Node B is selectively forwarding packets to Node C. Node A promiscuously listens to node B's transmissions.

In this paper, we propose a method that can detect black hole attack for secure data communication in wireless sensor network which uses watchdog technique. The rest of the paper is organized as follows: In section II Basic concept is discussed. Section III the previous work done by various authors in context with the security issues in WSN is discussed. Section IV develops the proposed intrusion detection algorithm. In section V, we present the simulations in the NS-2. Section VI concludes this paper.

3. Related Works

In recent years the importance of the security of wireless sensor networks has been extensively discussed and universalized. A technique has been applied to detect the black hole attack by eliminating the false route and updating the route table with avoidance of the overhead [9]. The concept of watchdog has been applied for the detection of malicious node [11].

The cluster head is assigned as a watchdog node which monitors the data traffic and detects the anomalous behavior of the compromised node. Multipath routing scheme can also be used as a security technique against selective forwarding attack [12]. With any packet drop the node will resend the packets from the substitute route. Such a method improves the safety of the network. In [13], a new scheme has been introduced for the detection of selective forwarding attack and black hole attack. The idea behind this scheme i.e. nodes examine their neighborhood and communicate with the adjacent neighbor for detection of malicious node. Such a scheme may help in reducing computational load on the analyzing node but the communication overhead will be highly increased. A novel approach for detection of sinkhole attack in WSN has been presented in [14].

The sender node sends the RREQ packet with a request for sequence number, if the node sends back its sequence number with RREP packets. The sender will match the sequence number which is stored in its routing table. If matches then the data packets will be transmitted else a sequence number will be assigned to that node. The node will enter the network only if it accepts the assigned sequence number. If not then the node is eliminated from network. An intrusion detection method for sinkhole attack has been proposed in [15] where the interested node will send a control packet in single hop to the main base station (BS) before sending the data packets. Then data packets are send in to the BS in hop by hop manner. On receiving data packets, BS compares some of its control fields to the field of stored control packets. If it does not match then malicious node is present. The propose method is applied to detect the presence of malicious node. In another work, two different solutions for illumination the problem of black hole attack have been proposed.

The first solution proposes multipath scheme having redundant paths at least three paths which must have some shared hops. In the next step, the source node unicasts a ping packet to the destination using these routes which contains different packet IDs and sequence number. The node will reply to this ping request if there is any route present for destination. The source will check those acknowledgements, and find out insecure path and malicious node. The second proposed solution maintains two tables for last received and last send packet respectively. Both tables are updated when RREQ and RREP messages are sent and the values are compared with the previously stored data in the tables. If both the value

matches then transmission occurs else the alarm is raised against replied node as malicious node.

4. Proposed Method

The existing mechanism has some limitations. Firstly, no communication will take place if no shared hops are present in between the routes. Secondly, the time delay increases as receiving and processing of RREP packets by source increases. Each node maintains supplementary table thus more memory space is required. The proposed method uses watchdog technique for detection. When a node sends a data, the selected watchdog node monitors the next node to verify that it also sends the data further. If watchdog node found any node not transmitting data further then that node is considered as a malicious node. The simple technique used by the watchdog node to detect the malicious node in the network by eliminating the false route entry.

The proposed method is divided into two phases: Initialization phase and Detection phase.

Initialization Phase: This phase deals with the selection of watchdog node. The node which is assign as the watchdog node is that node which is highly connected node (i.e. both in degree and out degree of a node) can be calculated by the neighbor table. Assuming that watchdog node cannot be a malicious node. The watchdog mechanism is periodically used in this work i.e. continuous monitoring does not require. Watchdog node will observed the end-to-end behavior of the node while communication.

***Detection Phase*:** For every threshold time t, the watchdog node searches for the malicious node. The watchdog node maintains three tables: route table, source and destination table. Route table is generated when the route is discovered from source to destination. When the packet sends from a source to destination node the source table is filtered by source entry in the Route Table as well as when the packet are sends back from destination to source node, at that time destination table is also filtered by destination entry in Route Table. The source and destination table consist source id, destination id, next- -hop, hop count and the sequence number. From these tables we get the information about the number of routes discovered from source to destination.

When the source broadcasts the RREQ packets to its neighbor node for route discovery of the destination; the watchdog node monitor the packets and generated source table for each packets. Every packet consist its unique sequence number (X). Each node send RREP packets which also consists unique sequence number(Y) and the destination table is generated by watchdog nodes which consists information about all the nodes RREP packets. If the sequence number of RREP packet (Y) is greater than the RREQ packet (X); then the route is updated. If the malicious node is present the sequence number of its packet is much greater say Y. As the sequence number is greater the node considered it to be valid and update the route. So that the malicious node is the first node to response, the routing table of node is updated with RREP information from node. The watchdog node to detect the malicious node uses the following rules:

1) For a given threshold time t, it analyzes the path found from source to destination. If the path found by the source and destination has the common nodes then no malicious node is present else the node which is uncommon in the path from whichever table may be malicious node
2) It checks the hop count of the nodes and the sequence number of the node. if hop count is 1 then its output(H) will be 1 else 0 and if sequence number is maximum then its output (Sn) will be as 1 else 0. Finally if the output is 1 then the node is malicious node.

hop count=H, Sequence Number=Sn, Output=Op.

```
L:
If (H= 1 || Sn = Max)
{
        Op= =1;
 }
Else
{
        Op= =0;
}
if ( Op= =1)
   {
  "Node is Malicious".
   }
Else
{
goto L;
}
```

If both conditions are satisfied as above then the node is considered as malicious node.

Sr. No	H (hop count)	Sn (Sequence no.)	Output
01	1	1	1
02	0	1	0
03	1	0	0
04	0	0	0

Now we present the algorithm with the following notation.

Notation: Rt =Route table, St=Source table, Se=Source entry, Dt=Destination table, De=destination entry, S=source, D=Destination, Qi=Common node.

Algorithm:

BEGIN

Initialization phase:

1. Create a topology T={q1,q2,q3,-------,q_n}
2. Select a watchdog node W from T (W € T).
3. W monitors the Network traffic.
4.

Detection phase:

5. For each threshold time (t) repeat Step-5 to Step-12.
6. Trace RREQ and RREP packets
7. Create Rt.
8. Filter St from Se in Rt.
9. Filter Dt from De in Rt.
10. Compare route given by S and D.
11. Search Qi.
12. If Qi present

    Then

        No malicious node present.

    Else

        Node is malicious.
13. Stop Simulation.
14. goto Step-3.

END

5. Simulation and Results

The proposed scheme is simulated in NS 2.35. The network is randomly distributed in an area of 750 m x 750 m and 20 nodes. The AODV routing protocol is used for communication. The simulation runs for 500 msec. The detection process is run for each threshold time of 5 msec. This simulation parameters used in our work as follows:

Sl No.	Parameters	Values
01	Number of Nodes	20
02	Simulation Time	500Ms
03	Pause Time	5Ms
04	Routing Protocol	AODV
05	Network Area	750 x750 M^2

We consider the following simulation metrics in our proposal:

1.) **Packet delivery ratio**: The ratio of the number of packet received to the number of packet send to the destination. This display the level of delivered data to the destination.

PDR= ∑ Number of packet receive / ∑ Number of packet send

The greater value of packet delivery ratio means the better performance of the protocol.

2.) **End-to-end Delay**: The average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

End-to-end delay= ∑ (arrive time – send time) / ∑ Number of connections

The lower value of end-to-end delay means the better performance of the protocol.

3.) **Data transfer rate:** the amount of data transfer in a given time.

Data transfer rate= amount of data /time

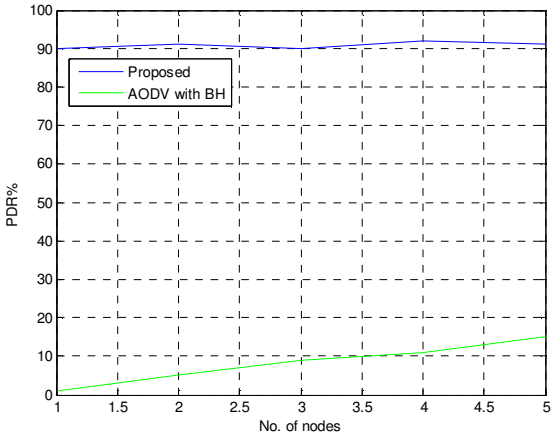


Figure 2

Figure 2 and 3 display the packet delivery ratio graph with respect to number of nodes and malicious node .The graph display that the packet delivery ratio of the proposed work is higher as compared to AODV protocol. On applying the proposed method the packet delivery is achieved 90%.

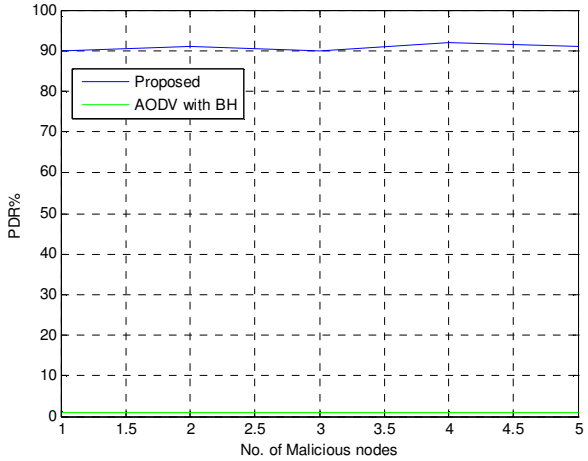


Figure 3

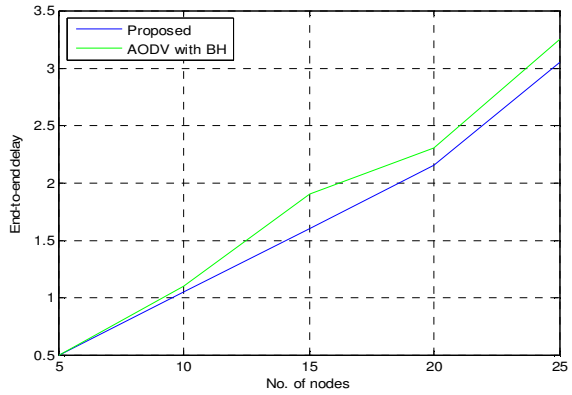


Figure 4

In figure 4, end-to-end delay graph is depicted. The graph display that the performance of the system increases by applying proposed method.

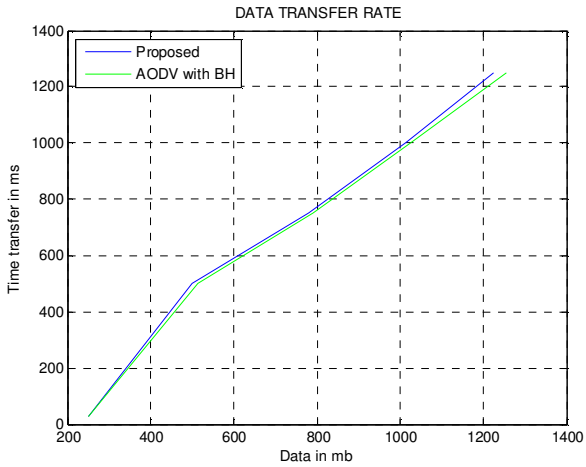


Figure 5

Figure 5 represents the rate of data transfer of both the system. AODV take more time to transfer data in comparison with the proposed model.

6. Conclusion

In this paper, we presented an effective method for detecting the black hole attack in a wireless sensor network. The watchdog technique is implemented in this work. The proposed model better improves the network performance by avoiding the malicious node from the network. Future work can be to focus on the detection of other attacks and comparison with black hole attack with different routing protocol. It may be categorized on the basis of how much they affect the performance of the network. The detection of other attacks as well as the elimination strategy for those attacks has to be carried out in future research.

References

[1] M. Tiwari, K.Veer Arya, R. Choudhari, K. Sidharth Choudhary, "Designing Intrusion Detection to Detect Black hole and Selective Forwarding Attack in WSN based on local Information", "*2009 Fourth International Conference on Computer Sciences and Convergence Information Technology*"

[2] E. Nam Huh and T. Hong Hai, "Lightweight Intrusion Detection for Wireless Sensor Networks"

[3] J. Du, J. Li, " A Study of Security Routing Protocol For Wireless Sensor Network", "*2011 International Conference on Instrumentation, Measurement, Computer, Communication and Control"*

[4] F. Bao, I. Ray Chen, M. Jeong Chang, and J.-Hee Cho, "Hierarchical Trust Management for Wireless Sensor Networks and its Applications to Trust-Based Routing and Intrusion Detection", *"IEEE Transactions On Network And Service Management, June 2012"*

[5] M. A. Rassam, M.A. Maarof and A. Zainal, "A Survey of Intrusion Detection Schemes in Wireless Sensor Networks", *"American Journal of Applied Sciences, 2012"*

[6] W. Ribeiro Pires J´unior, T. H. de Paula Figueiredo H. Chi Wong, A. A.F. Loureiro, "Malicious Node Detection in Wireless Sensor Networks", *"Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04),IEEE 2004*"

[7] V. K. Jatav, M. Tripathi , M S Gaur and V. Laxmi, "Wireless Sensor Networks: Attack Models and Detection", "*2012 IACSIT Hong Kong Conferences IPCSIT vol. 30 (2012) © (2012) IACSIT Press, Singapore*"

[8] A. Paula R. da Silva, M.H.T. Martins Bruno, P.S. Rocha, A. A.F. Loureiro, L. B. Ruiz, H. Chi Wong, "Decentralized intrusion detection in wireless sensor networks", "*Proceedings of the 1st ACM International Workshop on Quality of Service and Security in Wireless and Mobile Networks, 2005"*.

[9] G..Saravanan, P. R.Patil, M.R. Kumar, "Survey on Intrusion Detection System in Heterogeneous WSN Using Multipath Routing", "*IOSR Journal of Computer Engineering (IOSR-JCE) e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 2, Ver. I (Mar-Apr. 2014), PP 26-31*"

[10] K Abd. Jalil, Z. Ahmad, J. Lail Ab Manan , "Mitigation of Black Hole Attacks for AODV Routing Protocol", *"International Journal on New Computer Architectures and Their Applications (IJNCAA) The Society of Digital Information and Wireless Communications, 2011"*

[11] S. Nishanthi "Intrusion Detection in Wireless Sensor Networks Using Watchdog Based Clonal Selection Algorithm", "*International Journal of Research in Engineering & Advanced Technology, Volume 1, Issue 1, March, 2013*"

[12] Geethu P C, R. Mohammed A, "Defense Mechanism against Selective Forwarding Attack in Wireless Sensor Networks", "4th *International Conference on Computing, Communications and Networking Technologies-2013"*.

[13] Krontiris, I., T. Dimitriou and F.C. Freiling, "Towards intrusion detection in wireless sensor networks.", "*Proceeding of the 13th European Wireless Conference, 2007*".

[14] T. Singh, H. Kaur Arora "Detection and Correction of Sinkhole Attack with Novel Method in WSN Using NS2 Tool", "*International Journal of Advanced Computer Science and Applications, 2013*"

[15] M. Bahekmat, M. Hossein Yaghmaee, A. Sadat Heydari Yazdi, and S. Sadeghi, "A Novel Algorithm for Detecting Sinkhole Attacks in WSNs", "*International Journal of Computer Theory and Engineering, June 2012"*

[16] M. Al-Shurman and Seong-Moo Yoo, S. Park, "Black Hole Attack in Mobile Ad Hoc Networks", "*Association for Computing Machinery Southeast Conference, April 2004"*

[17] Kumar, V.: Simulation and Comparison of AODV and DSR Routing Protocols in MANETs, Master Thesis (2009).

[18] Ei Ei Khin and Thandar Phyu," IMPACT OF BLACKHOLE ATTACK ON AODV ROUTING PROTOCOL", "International Journal of Information Technology, Modeling and Computing (IJITMC) Vol. 2, No.2, May 2014."

[19] H.Debar,M Dacier and A.Wepsi, 1999,"Towards Taxonomy of Intrusion Detection System.Computer network,31:805-822.

[20] P.Butch and C.Ko "Challenges in Intrusion Detection for wireless Sensor Networks", In Proceeding of application and the Internet Workshop.2003 symposium on.pp.368378.2003".

[21] Ei Ei Khin and T.Phyu" Mitigating Scheme for Black Hole Attack in AODV Routing Protocol" ,International Conference on Advances in Engineering and Technology (ICAET'2014) March 29-30, 2014 Singapore.

[22] Ei Ei Khin and T.Phyu" Enhancing AODV Routing Protocol to Eliminate Black Hole Attack in MANET" International Journal of Computer Science and Business Informatics.

[23] M. Mohanapriya , Ilango Krishnamurthi" Modified DSR protocol for detection and removal of selective black hole attack in MANET", Computers and Electrical Engineering 40 (2014) 530–538

Author Profile:

Umashankar Ghugar received his B.E degree in IT from Orissa Utkal University in 2006 and M.Tech degree in Computer Science from Fakir Mohan University,Balasore in 2012.He has 07 years of Teaching experience and Now He is PhD Scholar in Computer Science subject in Berhampur University,Orissa. His research interests are in Computer Networks such as Wireless Sensor Network and Network security. He is currently a member of IACSIT, CSTA and IRED.He has published 02 International journal papers.

Dr.(Prof)Jayaram Pradhan started his teaching career as Computer Sc lecturer at Bhopal University in the year 1985 after completing M.Phil Computer Sc from J.N University New Delhi. He joined in the department of CSEA, REC Rourkela in the year 1986 where he completed his doctorial dissertation under Sambalpur University. In the year 1993 he joined in the department of Computer Science Berhampur University and worked as founder Head of the department.

During more than three decade experience he has offered different courses to DCA, MCA, BE, M.Tech students, beside guided many M.Tech, Ph.D scholars, published many papers, reviewed different manuscripts of journals, adjudicated several M.Tech/Ph.D thesis of other Indian University, design many courses, deliver several talk at different Universities with in India and abroad. Now He is the PG Council Chairman of Berhampur University,Orissa.In addition he has many academic administrative assignment during this period. His present research interests include Designing of Algorithms, Cryptography and computationally hard problems.

Dr.(Mrs)Monalisha Biswal received her PhD Sambalpur University,Orissa.Now she is working as a Asst Professor in NIR Raipur in Department of Electrical Engineering. She has published 17 International Referred journal papers. She is a Member of IEEE,Associate Member, The Institution of Engineers, India, Life Member of Orissa Bigyan Academy,ISTE, Life Member: LM-95003. Her research interests are power System Protection, Smart Grid Protection, Wide Area Protection, FACTS Devices, Adaptive Relaying, Signal Processing Application to Power System Relaying.