International Journal of Advanced Information Science and Technology (IJAIST) ISSN: 2319:2682
Vol.3, No.10, October 2014 DOI:10.15693/ijaist/2014.v3i10.125-131

CBIDS: **C**redit **B**ased **I**ntrusion **D**etection **S**ystem to Counter Black Hole Attack in Wireless Sensor Networks

Ranjeeth Kumar.S
Research Scholar/School of Computing,
SASTRA University, Tanjore, India

Umamakeswari. A
Associate Dean/Department of CSE,
SASTRA University, Tanjore, India

***Abstract*— Wireless networks follow Ad Hoc policy of topology formation, which makes them to expose many security vulnerabilities. These networks are more prone to security attacks, since it has no direct monitoring mechanism. The growing need in the security of wireless environment created more attraction to the researchers to involve in the research in the security of the wireless networks. The network layer in the protocol stack has more possible threats which include packet dropping, packet rerouting, eavesdropping etc. Black hole attack is a routing attack that deliberately drops all the packets that are received from the source node. The proposed Intrusion Detection System (IDS) namely Credit Based IDS uses a numeric value namely credit value. The Black hole node is identified using this credit value and the proposed work is simulated in NS2. The results verified that the throughput increased with our approach compared to the traditional Ad Hoc protocol.**

Index Terms: Wireless sensor networks, Black hole attack, Intrusion detection systems

I. INTRODUCTION

The security threats in wireless networks are classified into several types based on the factors like action, layers and location. Based on the action the attacks are divided into Active attacks and Passive attacks, wherein if the attacker makes any changes in the data or add any new information then it is called as **Active attack**. If the attacker simply eavesdrop the transmission, it is called as the **Passive attack**. Some of the examples for the active attack are Denial of Service (DOS), Selective forwarding, Black hole attack, Sinkhole attack, Sybil attack, etc. and Eavesdropping, Traffic analysis are few example of passive attacks. The attacks are classified depending on the location into two types like **Outsider attacks** and **Insider attacks**. The Outsider attacks are launched by the intruder by making the genuine nodes in the network as compromised nodes. Insider attack is launched by the nodes in the network. The layering is also a criterion to classify the threats. The research focus is on curbing and managing the routing layer threats in the wireless network. The attack occurs during the compromised node claiming to have the shortest path by sending a fake reply and drops all the packets once the traffic is redirected to this node. A credit based system is used to capture the Black hole attack considering AODV routing protocol. AODV protocol has two sections namely path discovery and maintenance. In the first section the process is started when the sender node discover the route to the receiver node. The second section is maintenance which includes packet transfer, packet rerouting and retransmission.

A. Black Hole attack

This is a routing layer attack and the compromised node will always do favorable reply to the sender informing indicating the shortest path. The malicious node will pretend that it is the nearest neighbor and falsify the sender towards forwarding the information to it. The sender node transmits the packet to the malicious node considering it as a genuine member. The attacker node receives the data from the sender node and drops the entire set of data packets and doesn't forward to the intended node. Since the compromised node consumes the packets, it is called as Black Hole node in relating to Black Hole region in the space which is believed that all the objects passing through that region will disappear. The Black Hole attack is said to be most dangerous security threat to the sensor network since it drops all the data packets. Mitigating and preventing the Black Hole attack is a challenging task with minimum resource constraints of sensor networks. This work concentrate on the Black Hole attack on the Ad-hoc protocol and the security mechanism is provided to mitigate the attack. The protocol is explained in the next section.

B. AODV Protocol

This is a routing protocol that builds the route as indicated or demanded by the source node. This protocol performs both Unicasting and Multicast routing Sender node sends the request packet (RREQ) to the remaining nodes in the network, which in turn update their routing tables and place their backward pointers towards the sender node. The request (RREQ) packet contains the source IP, sequence number and broadcast Identification number. The nodes which receive the RREQ message should reply to the sender node when there is a route to the final node through unicasting method, otherwise it rebroadcasts the request packet to the others in the network.

The source node collects the forward pointer information and transmits the data to the final node and if the sender gets an RREP message from a node N then it checks whether the sequence number of the sensor node N is greater or similar with least hop count and update its routing information. The source node sends the packets as long as the route is active, if link break is happened during the transmission the node in the upstream inform the source about the unreachable status through an error message (RERR).The source node after receiving the error message can initiate route discovery process. This article is structured as below, first the similar work for Intrusion detection, second the proposed algorithm, third about implementation, fourth it discusses the results and fifth conclusion and future work are discussed.

II.RELATED WORK

Many research works in WSN focus on developing the security algorithms for mitigating the Black Hole attack and some of the recent works are discussed in this section. The survey article by I.F. Akyildiz et.al., [1] about wireless sensor networks (WSN) give the complete fundamental aspects. The protocol stack of WSN is explained along with the security, energy efficiency and other characteristics in a detailed manner which helps the researchers to know the basic structure and problems of wireless sensor networks. The BAMBi is an intrusion detection method proposed by S.Misra et.al [2] to detect the black hole attack with having more than one base station. This method consumes more energy due to the presence of multiple base stations. M.A.Shurman et.al [3] proposed a method in which the source node provides authentication. In this method the routing delay is high and makes unsuitable for WSN. Zdravko Karakehayov [4] proposed REWARD protocol for detecting the black hole attacks in wireless sensor networks. This protocol uses two messages MISS and SAMBA and have a database to store the route. This protocol may increase the communication overhead and storage. Jaydip Sen [5] introduced a detection mechanism to detect cooperative black hole attack in WSN, but the computation overhead is higher when compared to other methods. Juan-Carlos et.al [6] proposed method for the black hole attack in Mobile Ad-hoc Network, but the security mechanism is not developed. Md. Amir Khusru Akhtar1, G. Sahoo [7] proposed a behaviour monitoring protocol namely BBHP is compared to I-MAN and need to be compared to other behavior monitoring protocols. This BBHP method mitigates black hole attack and other threats. Hongmei Deng et.al [8] proposed method to disable the replaying of the intermediate node and has two disadvantages, routing delay is increased and malicious node can fabricate the reply message of the final node. Wenchao Li et.al [9] proposed KNN algorithm for finding the abnormal nodes from the normal nodes using the AODV protocol against flooding attack. If the cutoff rate is not appropriate it will increase the error rate of the detection. This method uses K-distance function and cutoff value for identifying the abnormal nodes. Sathoshi Kurosawa et.al.[10] presented a learning method which is of dynamic in nature for detecting the black hole attack on the AODV protocol. This method doesn't address the cooperative black hole attack. L.Raja, Dr. S. Santhosh Baboo [11] analysed the black hole attack on Ad-Hoc protocol by explaining the impact of fake RREQ and RREP message. Jaspal Kumar, M. Kulkarni, Daya Gupta [12] proposed improved version of AODV namely IAODV which mitigate the black hole attack. The communication overhead is high in IAODV compared to traditional AODV method. The packet delivery ratio is approximately same in both AODV and IAODV under black hole attack. Dr.Tamilarasan [13] proposed a method called prior-receive reply which contains the new table, timer and malicious node ID. The simulation result of this algorithm doesn't take the overhead as a metric and feasibility of this algorithm towards the communication overhead is an issue. Sanjay Ramaswamy et.al. [14] Introduce Data Routing Information table (DRI) and cross checking to traditional AODV to solve the combined black hole attack. This method depends on reliable node and if it is compromised then the black hole nodes cannot be identified and the cost of the cross checking mechanism is little high which can be identified as the drawbacks. Ramasamy Murugan and Arumugam Shanmugam [15] proposed timer based acknowledgement scheme for detecting the misbehaving nodes. The timer value is recorded for both forwarding and receiving the packets for each node. If the values are same then the node is genuine or else it is a malicious node. Chong Eik Loo et.al. [16] Proposed IDS which run on each sensor node to capture the anomalies by analysing the traffic features. Periodic route error attack and Sinkhole attack is tested but remaining routing attacks are not analysed.

III. IMPLEMENTATION

Sender node sends the route request packet to the neighboring nodes to find the route to the final node. Consider a compromised node lies in the intermediate path, then it falsely send route replies (RREP) to the sender node without forwarding the request packet to its neighbor nodes to capture the network traffic and drops all the packets. A senor network is created with few nodes in which node 5 is considered as the source node and other (in this case 9) as the destination node. **Figure 1** depicts the creation of a network with the malicious node. The compromised node i.e, in our case, the black hole node is injected into the network. This operation is performed by either an insider or outsider. The black hole node is created successfully and the network is modified to an abnormal condition. Once a node in the network is compromised by the attacker, then he can successfully drop all the packets and make the network to be collapsed. The compromised node is not known to the other nodes, so it starts continuously send the

packets. The normal node doesn't know the dropping of packets and keep on sends the packets. In this Figure 1 the node which is given black color indicates the presence of the black hole node.

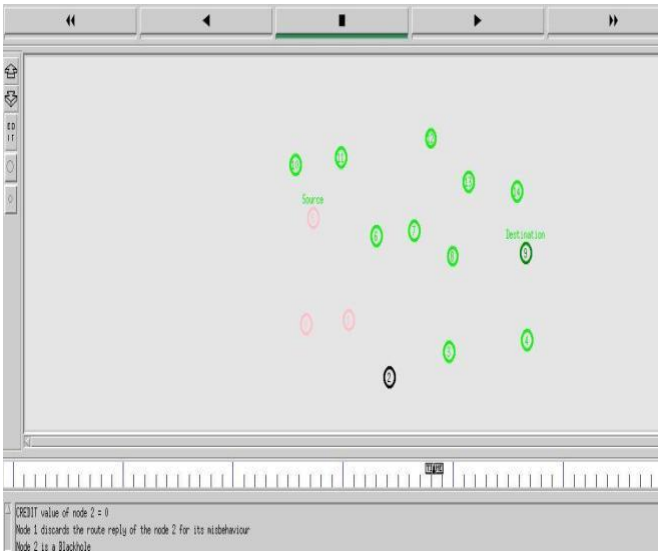

Figure 1. Black hole Injection.

Figure 2 shows the node with identification number 2 as the malicious node for packet dropping that travel across its way towards destination.

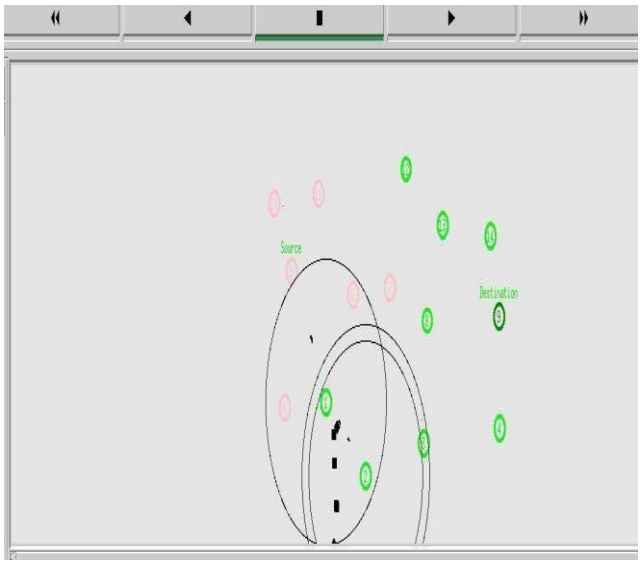

Figure 2. Packet Dropping.

A. Algorithm Description

Algorithm CBIDS( )

1) **Begin:**

2) **Assumptions:**

Let n1,n2…..n_k be the nodes in the sensor network(sn) where $\forall\ n_i \in sn_i$ i.e., i=1,2,…..n and src be the source node in the network

Let T_i be the node information table with the fields like Node identification number (Ni),

Neighbor node identification number (NNi), Forwarding node credit value (cv_{fi}), Replying node credit value (cv_{ri})

3) Repeat

4) src forwards the route request packet

(RREQ) to the neigbour node N_i

5) cv_{fi}++

6) Update the values in the table T_i

7)Until the reply message (RREP) is

received

8) If (cv_{ri} != 0)

9) broadcast the alert signal with N_i as

the malicious node

10)else

11) src forwards the data to the destination

12) End

Initially the credit value of all the nodes should be zero and every time when a sender node sends the route request packet to its neighbor, the credit value of the source node increases by the value one. This implies that the credit value of the node is actually equal to the number of its neighbors. The basic approach is to analyze the credit value of a sensor node which sends the RREP packet. If any of the sensor node replies for the request message, then its credit value is checked, since the destination node doesn't forward any RREQ packet, its credit value will be always equal to 0. If the credit value of the replying node is non-zero then an alert signal is broadcasted to all other nodes declaring it as a malicious node. The compromised node is eliminated from the transmission and other nodes keep sending the RREQ to its other neighbor nodes until a real destination node sends the route reply message. The RREP message is transmitted from secure neighbors to the source node which in turn sends the data through these secure neighbors to the destination node. **Figure 3** shows an alternate path to the final node.

IV. RESULTS AND DISCUSSION

A. Pre-CBIDS Implementation

The proposed algorithm is simulated in the Network Simulator (NS2). The parameters taken for the comparison of the traditional AODV and the CBIDS implemented AODV are packet drop ratio, packet delivery ratio and throughput. The xgraph tool is used to generate the graph with this parameters and the algorithm is implemented. The results are categorized into two sections.

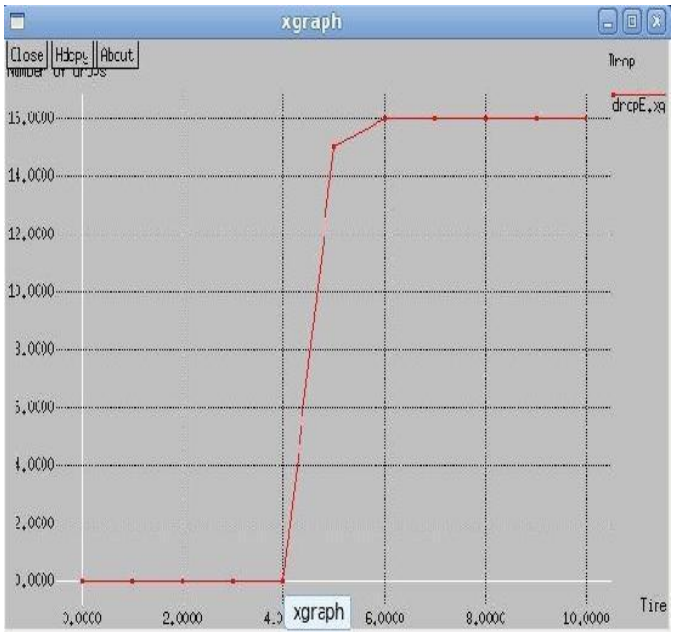

Figure 4. Packet drop rate

The first section show the graphical comparison of the values for the Traditional AODV implementation and the next section shows the value comparison after the implementation of the CBIDS algorithm. In the above **Figure 4** shows the red line which indicates the drop rate of the traditional AODV with a malicious node. The drop rate gradually increases after the intervention of the black hole node in accordance with the time and it reaches peak in an exponential rate.

Figure 5 shows the steady degradation of throughput in the traditional AODV when the black hole node injection is performed. This depicts the drastic change of the black hole threat over the data transmission. The presence of the black hole node will make the throughput to reach almost to zero. Since the black hole node drops all the packets which it receives from the neighbors, the destination node doesn't receive any packets which make the throughput value to reach 0. Throughput is a important metric to calculate the network efficiency and in the presence of a black hole node it is reduced to an unacceptable level.

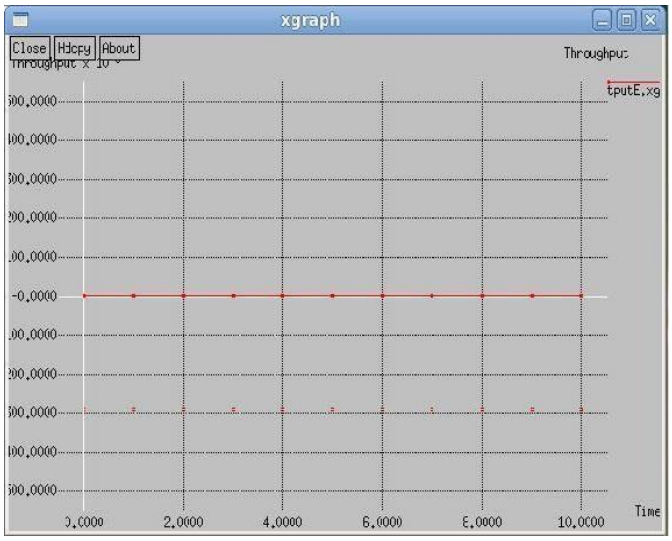

Figure 5. Throughput

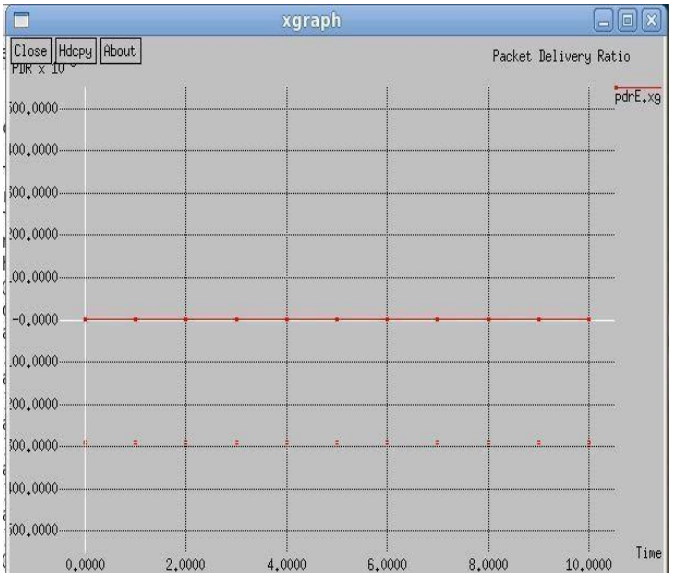

Figure 6. Packet delivery ratio

Figure 6 shows how the packet delivery ratio is reduced to a greater extent due to the packet dropping by the compromised node. The compromised node drops the packets in the traditional AODV protocol which show a greater reduction in

the packet delivery ratio. The PDR is decreasing in proportion with the time of the process.

B. Post-CBIDS Implementation

The CBIDS algorithm is implemented in the traditional AODV protocol and the results are verified. The black hole node is detected at the earliest stage and the comparison parameters show the significant improvements in the traditional protocol. **Figure 7** show the red line indicates the traditional AODV protocol (dropE) which shows the steady increase in the packet drop rate due to the malicious node. The green line indicates the improvement of the traditional AODV protocol after implementing the CBIDS algorithm (dropP). **Figure 7** show the red line indicates the traditional AODV protocol which shows the steady increase in the packet drop rate due to the malicious node. The green line indicates the improvement of the traditional AODV protocol after implementing the CBIDS algorithm. The malicious node is detected at the earliest point and the packet drop rate is almost equal to 0.

Figure 7.dropE vs. dropP

Figure 8 shows the CBIDS algorithm is implemented and the information about the black hole node is broadcasted to all other nodes (pdrP). The packet delivery ratio is almost 100% after the detection of the black hole node. The red line indicates the traditional AODV (pdrE) which suffers from the heavy packet loss i.e., all the data packets are dropped due to the presence of the black hole node. The detection of the black hole node makes the packet dropping reduced. When the compromised node is detected and informed to the neighbours,

then it realizes and stops forwarding the packets to the black hole node which make the packet drop ratio to zero. If the compromised node is not detected then the packet drop ratio reaches the maximum leaving the network unstable. The CBIDS algorithm identifies the black hole node and immediately broadcast the black hole node information to the neighbours and alerts to avoid packet dropping.

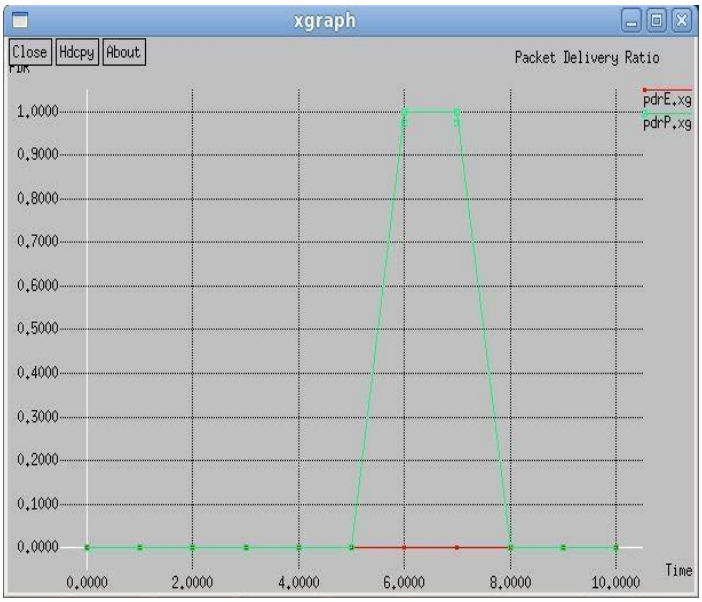

Figure 8. pdrE vs. pdrP

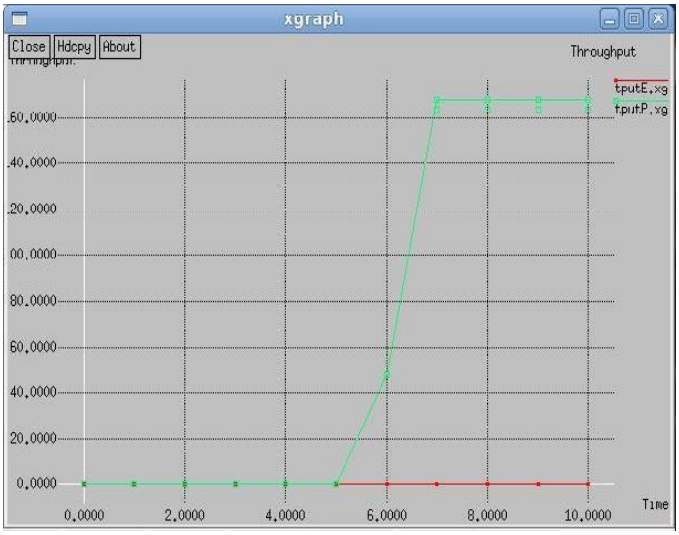

Figure 9. tputE vs tputP

Figure 9 shows the black hole injected network with traditional AODV protocol (tputE) is suffering from very low throughput wherein the CBIDS implemented network (tputP) has a gradual increase in the throughput and it reaches the maximum after the elimination of the black hole node. This proves the effectiveness of our CBIDS algorithm over the traditional Ad-Hoc protocol which is affected by the security attack.

V. CONCLUSION AND FUTURE WORK

The black hole node had been successfully detected in the wireless sensor network and the packets are re-routed through another path and a warning message has been broadcasted to the neighbouring nodes about the malicious node and further communication to that node is avoided. This CBIDS method used local information in order to solve the threat caused by the malicious node to the network and this method increases the energy efficiency since it reduces the communication overhead. This security mechanism can be extended towards the cluster of nodes and possibly the CBIDS can be kept at the cluster head and it can monitor the network for any presence of the black hole nodes.

ACKNOWLEDGEMENT

We are grateful to the Management of SASTRA University for providing all types of support in conducting this research activity. This research is carried out with the help of fund supported by the SASTRA University.

REFERENCES

[1] I.F.Akyildiz et.al, "Wireless sensor networks: a survey," *Computer Networks*, Vol.38, no.4, pp.393-422, 2002.

[2] Misra S et al, "BAMBi: Black hole attacks Mitigation with Multiple Base stations in Wireless Sensor Networks," in *Proceedings of the IEEE ICC, 2011.*

[3] Shurman M A et al, "Black hole attack in Wireless ad hoc networks," *Proceedings of 42nd ACM Southeast conference (ACMSE'04), 96-97, 2004.*

[4]Zdravko Karakehayov, "Using REWARD to detect team black-hole attacks in wireless sensor networks," *Proceedings of the workshop on Real-World Wireless Sensor Networks REALWSN*, 2005.

[5] Jaydip Sen, "Detection of Cooperative Black Hole Attack in Wireless Ad Hoc Networks," *International Journal of Simulation, Systems, Science and Technology*, Vol.12, no. 4, 2012.

[6] Juan-Carlos et.al, "Black Hole Attack Injection in Ad Hoc Networks," *Proceedings of International Conference on Dependable Systems and Networks*, 2008.

[7] Md.Amir Khusru Akhtar, G.Sahoo, "Behavior Based High Performance Protocol for MANET," *Indian Journal of Science and Technology*, Vol. 6, no. 10, 2013.

[8] Hongmei Deng, Wei Li and Dharma P.Agrawa, "Routing Security in Wireless Ad-HocNetworks," *IEEE Communications Magazine*, 2002.

[9] Wenchao Li et.al., "A New Intrusion Detection System Based on KNN Classification Algorithm in Wireless Sensor Network", *Journal of Electrical and Computer Engineering,* Vol.2014, 2014.

[10] Sathoshi Kurosawa et.al, "Detecting Black hole attack on AODV-based Mobile Ad-Hoc Networks by Dynamic Learning Method," *International Journal of Network Security,* Vol.5, no.3, pp.338-346, 2007.

[11] Raja L,Santhosh Baboo S, "Analysis of Blackhole Attacks on AODV Routing Protocol in MANET," IJCSET, Vol.2, pp. 1522-1526, 2012.

[12] Jaspal Kumar, Kulkarni M, Daya Gupta, "Effect of Black Hole Attack on MANET Routing Protocols," *International Journal of Computer etwork and Information Security*, Vol.5, pp. 64-72,2013.

[13] Tamilarasan S, "Securing and Preventing AODV Routing Protocol rom Black Hole attack using Counter algorithm," *International Journal of Engineering Research & Technology*, 2012.

[14] Sanjay Ramasamy et.al, "Prevention of Cooperative Black Hole attack in Wireless Ad-Hoc Networks," *Proceedings of International Conference on Wireless Networks*, 2003.

[15] Ramasamy Murugan, Arumugam Shanmugam, "A timer Based Acknowledgement Scheme for Node is behavior Detection and Isolation in MANET," *International Journal of Network Security,* Vol.15, no.4, pp.241-247, 2013.

[16] Chong Eik Loo et.al., " Intrusion Detection for Routing Attacks in Sensor Networks," *International Journal of Distributed Sensor Networks,* Vol. 2, no. 4, pp.313-332, 2006.

Authors Profile

Ranjeeth Kumar started the basic degree in computer science in Jawahar Science College, Neyveli, Tamilnadu, India. He completed the Master degree in computer technology from Coimbatore Institute of Technology, Coimbatore, Tamilnadu,

India and a Master degree in computer science and engineering from Pavendar Bharathidasan College of Engineering and Technology, Trichirappalli, Tamilnadu, India. He has 4 years of teaching experience in engineering institutions and participated in several conferences and workshops. He published one research paper in international conference and participated in young IT professional competition conducted by CSI India. He is currently a research assistant in SASTRA University, Thanjavur, Tamilnadu, India. His research interests are Network security, Wireless Sensor networks, Cloud Computing, Internet of Things and Objected Oriented Design.

Dr.A.Umamakeswari is currently working as Associate Dean in the Department of Computer Science and Engineering, School of Computing, SASTRA University, Thanjavur. She received her Bachelor's degree in Engineering from A.C.C.E.T., Karaikudi in 1989, Masters Degree in 1994 from NIT (formerly REC), Trichy and Doctorate from SASTRA University in 2009. She has 25 years of work experience and her research interests are in the area of Computer Vision, Embedded Systems, Wireless Sensor Networks and Software Engineering. She has presented papers in Conferences and published papers in reputed Journals. She has done collaborative projects and also organized international conferences.