A MECHANISM FOR DETECTION AND PREVENTION OF MULTIPLE GRAY HOLE ATTACK IN WIRELESS SENSOR NETWORKS

Ankita Rana[1],Er. Ankita Mittal[2]

[1] Student,CSE,Galaxy Global group of Institutions, Sahabad Markanda, Haryana, India
[2] Assistant Professor, CSE,Galaxy Global group of Institutions, Sahabad Markanda, Haryana, India

ABSTRACT

In the current decade, wireless sensor networks are emerging as a peculiar multi-disciplinary research area. Wireless Sensor Networks (WSNs) are appealing to researchers due to their wide range of application potential in areas such as military purposes, environmental monitoring and gathering information in inhospitable locations. Wireless Sensor Networks are dense wireless networks of small, low-cost sensors, which collect and disseminate environmental data. Sensor networks vary in size and can consist of 10 to 1,000,000 sensor nodes. Sensor nodes used to form these networks are resource-constrained, shich makes these types of security applications a challenging problem. A basic technique to protect data is encryption; but, due to resource constraints, achieving necessary key agreement for encryption is not easy. Watchdog mechanism proposed in is a monitoring method used for wireless sensor networks, and is the basis of many misbehavior detection algorithms and trust or reputation systems. In this paper, the behavior of multiple gray hole attacks and the performance impact of this attack on AODV protocol and its counter measures using Watchdog AODV scheme is studied. The NS2 network simulator is used for evaluation.\

Keyword: - *WSN, AODV, MAC.*

1. INTRODUCTION

Wireless Sensor Networks (WSN) Sensor networks represent a new frontier in technology that holds the promise of unprecedented levels of autonomy in the execution of complex dynamic missions by harnessing the power of many inexpensive electromechanical microdevices. The primary component of the *network* is the sensor, essential for monitoring realworld physical conditions or variables such as temperature, humidity, presence/absence, sound, intensity, vibration, pressure, motion, and pollutants, among others, at different locations. The basic goals of a WSN are to determine the value of physical variables at a given location, detect the occurrence of events of interest, and estimate parameters of the detected event or events, classify a detected object, and track an object []. Thus, the important requirements of a WSN are low energy consumption, self-organisation capability, collaborative signal processing, and querying ability. In order to keep their cost low, the sensors are equipped with limited energy and computational resources. The energy supply is typically in the form of a battery and once the battery is exhausted, the sensor is considered to be dead. The nodes also have limited memory and processing capabilities. Hence, harnessing the potential of these networks involves tackling a myriad of different issues from algorithms for network operation, programming models, architecture and hardware to more traditional networking issues. There are several key components that make up a typical wireless sensor network (WSN) device. General architecture of a wireless sensor device is, as shown in figure 1.

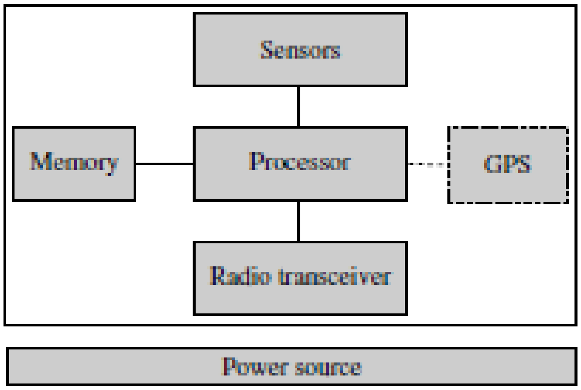

Figure 1: General Architecture of a Wireless Sensor device[].

Wireless sensor networks promise an unprecedented fine-grained interface between the virtual and physical worlds. They are one of the most rapidly developing new information technologies, with applications in a wide range of fields including industrial process control, security and surveillance, environmental sensing, and structural health monitoring. Because of their pervasive and sometimes critical surveillance operation, the data collected by sensor networks must be kept private, and networks must also be protected against malicious attacks aimed at disrupting or disabling their functionality. Security is the combination of processes, procedures, and systems used to ensure confidentiality, authentication, integrity, availability, access control, and non repudiation.

Confidentiality is to keep the information sent unreadable to unauthorized users or nodes. WSN uses an open medium, so usually all nodes within the direct transmission range can obtain the data. One way to keep information confidential is to encrypt the data, and another technique is to use directional antennas.

Authentication is to be able to identify a node or a user, and to be able to prevent impersonation. In wired networks and infrastructure-based wireless networks, it is possible to implement a central authority at a point such as a router, base station, or access point. But there is no central authority in WSN, and it is much more difficult to authenticate an entity.

Integrity is to be able to keep the message sent from being illegally altered or destroyed in the transmission. When the data is sent through the wireless medium, the data can be modified or deleted by malicious attackers. The malicious attackers can also resend it, which is called a replay attack.

Non-repudiation is related to a fact that if an entity sends a message, the entity cannot deny that the message was sent by it. By producing a signature for the message, the entity cannot later deny the message. In public key cryptography, a node A signs the message using its private key. All other nodes can verify the signed message by using A's public key, and A cannot deny that its signature is attached to the message.

Availability is to keep the network service or resources available to legitimate users. It ensures the survivability of the network despite malicious incidents.

Access control is to prevent unauthorized use of network services and system resources. Obviously, access control is tied to authentication attributes. In general, access control is the most commonly thought of service in both network communications and individual computer systems.

The network infrastructure of a WSN is made up of small, cheap nodes spread over a possibly hostile area. Unlike other types of networks, it is often impossible to prevent the sensor nodes from being physically accessed by attackers. This is also referred to as *node capture*. It is reasonable to assume that an attacker can achieve full control over a captured node, that is he can read its memory or influence the operation of the node software. Special secure memory devices would be needed to prevent the attacker from reading the memory; however, these will only rarely be present in cheap sensor nodes. The constraints regarding memory and computational capabilities are a serious obstacle for implementing cryptographic algorithms. Especially asymmetric key cryptography is considered too heavyweight for small processors, let alone the key management involved. When in-network processing is to be performed, intermediate nodes need to access and modify the information contained in packets; hence, a larger number of parties is involved in end-to-end information transfers.

. Avariety of attacks are possible inMANET. Some attacks apply to general network, some apply to wireless network and some are specific to MANETs. These security attacks can be classified according to different criteria, such as the domain of the attackers, or the techniques used in attacks. These security attacks in MANET and all other networks can be roughly classified by the following criteria: passive or active, internal or external, different protocol layer, stealthy or non-stealthy, cryptography or non-cryptography related.

Passive vs. active attacks: The attacks in MANET can roughly be classified into two major categories, namely passive attacks and active attacks. A passive attack obtains data exchanged in the network without disrupting the operation of the communications, while an active attack involves information interruption, modification, or fabrication, thereby disrupting the normal functionality of a MANET.

Internal vs. external attacks: The attacks can also be classified into external attacks and internal attacks, according the domain of the attacks. External attacks are carried out by nodes that do not belong to the domain of the network. Internal attacks are from compromised nodes, which are actually part of the network. Internal attacks are more severe when compared with outside attacks since the insider knows valuable and secret information, and possesses privileged access rights.

Attacks on different layers of the Internet model: The attacks can be further classified according to the five layers of the Internet model.

Stealthy vs. non-stealthy attacks: Some security attacks use stealth, whereby the attackers try to hide their actions from either an individual who is monitoring the system or an intrusion detection system (IDS). But other attacks such as DoS cannot be made stealthy.

Cryptography vs. non-cryptography related attacks: Some attacks are noncryptography related, and others are cryptographic primitive attacks.

Table 1 : Attacks on different layers of the Internet model.

Layer	Attacks
Application layer	Repudiation, data corruption
Transport layer	Session hijacking, SYN flooding
Network layer	blackhole, Grayhole, flooding, resource consumption, location disclosure attacks
Data link layer	Traffic analysis, monitoring, disruption MAC (802.11), WEP weakness
Physical layer	Jamming, interceptions, eavesdropping
Multi-layer attacks	DoS, impersonation, replay, man-in-the-middle

2. Related Work

S. Dai et al. [1], summarized recent research results on data routing in WSN and classified the approaches into three main categories, namely data-centric, hierarchical and location-based. Few other protocols followed the traditional network flow and QoS modeling methodology. Their study also observed that there are some hybrid protocols that fit under more than one category. The most interesting research issues in their study related to routing protocols for WSN are how to form the clusters so that the energy consumption and contemporary communication metrics such as latency are optimized, the consideration of node mobility, and integration of WSN with wired networks (i.e. Internet).

In Ref. [2], Huan Pham et al. present a new adaptive mobility-aware Sensor MAC protocol (MS-MAC) for mobile sensor applications. In MS-MAC protocol, a node detects its neighbor’s mobility based on a change in its received signal level from the neighbor, or a loss of connection with this neighbor after a timeout period. By propagating mobility presence information, and distance from nearest border node, each node learns its relative distance from the nearest mobile node and from nearest border node. Depending on the mobile node movement direction, the distances from mobile and border nodes, a node may trigger its neighbor search mechanism to quicken the connection setup time.

In Ref. [3], authors present MMAC, a mobility-adaptive, collision-free MAC protocol for mobile sensor networks. MMAC caters for both weak mobility (e.g. topology changes, node joins and node failures) and strong mobility (e.g. concurrent node joins and failures, and physical mobility of nodes). Finally authors point out that this protocol adapts the time frame, transmission slots, and random-access slots according to mobility.

P. Jiang1 et al. [4], gives a short overview of recent routing protocols for sensor networks and presents a classification for the various approaches. The four main categories studied in their paper are data-centric, hierarchical, location-based, and network flow and QoS-aware. Then, the existing hardware research platforms are explored as well as the software platforms such as simulation and development tools. Although the performance of these protocols is promising in terms of energy efficiency, further research would be needed to address issues such as Quality of Service (QoS). Another interesting issue for routing protocols is the consideration of node mobility. New routing algorithms are needed in order to handle the overhead of mobility and topology changes in such energy constrained environment. Since the routing requirements of each environment are different, further research is necessary for handling these instances.

Onkar V.Chandure et al. [5], describe the basic idea related with the implementation of AODV protocol and evaluates the impact of gray hole attack on adhoc network. A Gray hole is a node that selectively drops and forwards data packets after advertises itself as having the shortest path to the destination node in response to a route request message. The authors analyse the impact of gray hole attack on adhoc network for different performance metrices like packet delivery ratio and end to end delay. Simulation of AODV as well as gray hole attack is carried out by using ns-2 simulator.

Chetan S. Dhamande et al. [6], presented a brief study on different for the minimizing the impact of gray hole attack using AODV routing protocol.. Gray hole attack ultimately decrease the performance of the network & also corrupt the data Proposed solution is mainly focus on the miminize the impact of gray hole attack in MANET & also improve the security as well as the performance of the network. A gray hole may exhibit its malicious behavior in different ways. It may drop packets coming from or destined to certain specific node(s) in the network while forwarding all the packets for other nodes. Another type of gray hole node may behave maliciously for Some time duration by dropping packets but may switch to normal behaviour later.

Tarun Varshney et al. [7], investigate more existing mechanisms to prevent blackhole attack and propose a slight modification to AODV, called Watchdog –AODV (WAODV) that detects blackhole attack and also attempt to reduce further rise in normalized routing overhead. This mechanism firstly detects a blackhole node and provide a new route to source node. This mechanism greatly increases reliability of detection and isolation of multiple malicious blackhole nodes during route discovery process and discovers a short and secure route towards destination without introducing additional control packets.

Adnan Ahmed et al. [8], comprehensively investigates the performance of AODV protocol by simulating it on the various network parameters with various number of blackhole nodes.

AODV is source initiated, reactive and loop free routing protocol which creates route between source and destination when needed. AODV differs from its counterpart proactive routing protocols since in proactive routing updates are send periodically that leads to high overhead. The authors evaluates the performance of AODV routing protocol in presence of various number of blackhole nodes using Network Simulator 2 (NS2). The performance analysis is performed with the four conditions. First, there is no blackhole node in the network. Second, 1 node is compromised.· Third, there are two nodes thatbehave as blackhole nodes· Fourth, there are three nodes behave as blackhole nodes. The authors have compared AODV with compromised AODV in terms of normalized routing load, packet delivery ratio, end to end delay and packet drop ratio.

Smita Karmakar et al.[9], present a brief comparative study of various types of holes and various types of coverage holes. Holes are one of the challenges in deployment of WSNs in a large area. Holes generally considered as a communication gap among sensor nodes. The authors also provides a brief overview two different solutions for hole detection that are proposed by researchers. They are vornoi diagram and triangular oriented diagram. Voronoi diagram approach is used to detect a coverage hole and calculate the size of a coverage hole. A plane area is divided into N cells. Each cell contains one sensor. Two Voronoi cells meet along a voronoi edge. A sensor node is a voronoi neighbour of other sensor node, if they both share a voronoi edge. Voronoi diagram approach has few limitations like shape of each cell is different. So, it is very tough to calculate the exact size of the hole. The limitation of other solution namely triangular oriented structure is that, it is not a proper hole detection solution because, in a large WSNs, it is complex to connect the centre of three adjacent sensors. Here authors also proposed simple and straight-forward algorithm initially find out whether a sensor node is alive or dead. According to this algorithm, when the sensor node is dead, then the geographical area is not covered by that sensor node, so this area will be treated as hole.

Benamar Kadri et al. [10], propose a lightweight implementation of public key infrastructure called cluster based public infrastructure (CBPKI). CBPKI is based on the security and the authenticity of the base station for executing a set of handshakes intended to establish session keys between the base station and sensors over the network used for ensuring data confidentiality and integrity. CBPKI is intended to establish security over the network using three cryptographic methods destined to establish all the security services. CBPKI is based on two handshakes namely Cluster-head to base station handshake and Cluster members handshake. The handshake is executed by each cluster head and the base station is intended to establish a symmetric key be-tween sensors and the base station. propose to launch periodically a proactive key update of the session key; the period of the key update is defined by the administrator according to the length of the used keys as well as the robustness of the encrypting algorithms. The key update is launched by the cluster head using the same hand shake defined above in order to establish a new session key between the base station and the cluster head. After updating the session key of the cluster head, each cluster head encrypts a copy with the old session key for each member of its cluster. The authors also ensures the CBPKI for all security services and checks its robustness against several attacks with low power consumption and network overhead.

3. SIMULATIONS AND RESULTS

In this paper, we evaluate the performance of AODV routing protocol under Grayhole and counter measures it using Watchdog AODV.

Table 2: Simulation Scenarios

Cases	AODV	Under Grayhole-Attack	Under Modified Watchdog IDS System
Parameters			
No. Of attackers	Nil	3	3
Communication distance	110, 130, 150, 170 and 190 meters	110, 130, 150, 170 and 190 meters	110, 130, 150, 170 and 190 meters
No. of Police nodes	Nil	Nil	ALL

Simulations are performed for Gray hole attack in wireless sensor network environment. The impact of node's communication range on the performance of AODV routing protocol under Gray hole security attacks is shown with the help of simulation graphs in terms of remaining energy, Distinct event delivery ratio, and number of collisions

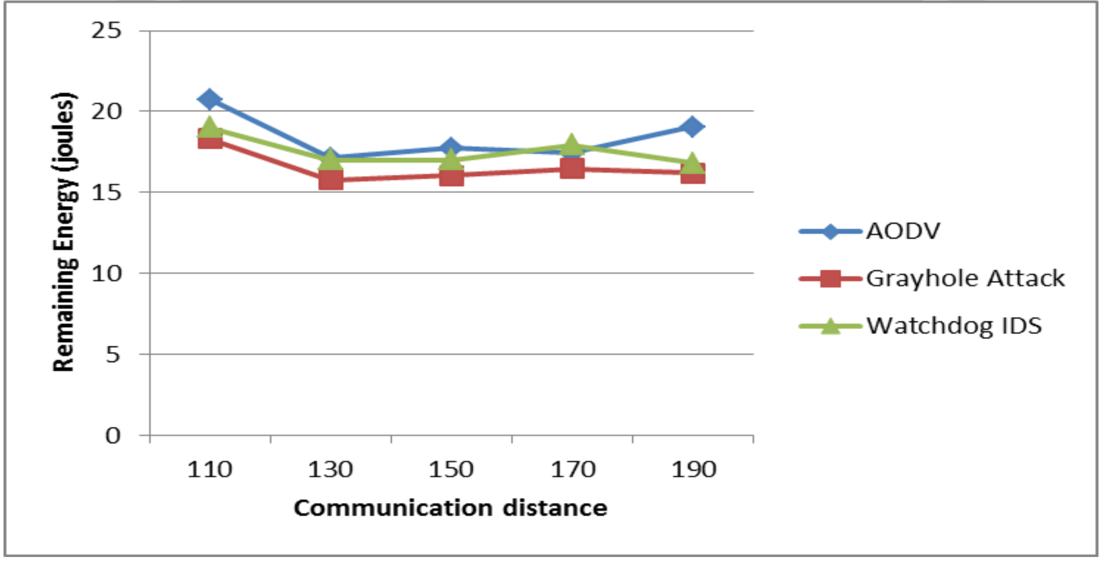

Figure 2: Remaining Energy versus Communication distance..

- Remaining Energy

Figure 2 shows the simulation graph for AODV routing protocol under gray hole attack and its proposed prevention mechanism namely watchdog intruder detection scheme in terms of the measured average remaining energy of sensors nodes when communication distance is varied between 110 to 190 meters. From the analysis of simulation graph, it is cleared that total energy consumption of AODV under gray hole attack is higher as compare to the total energy consumption of AODV along with watchdog intruder detetction scheme

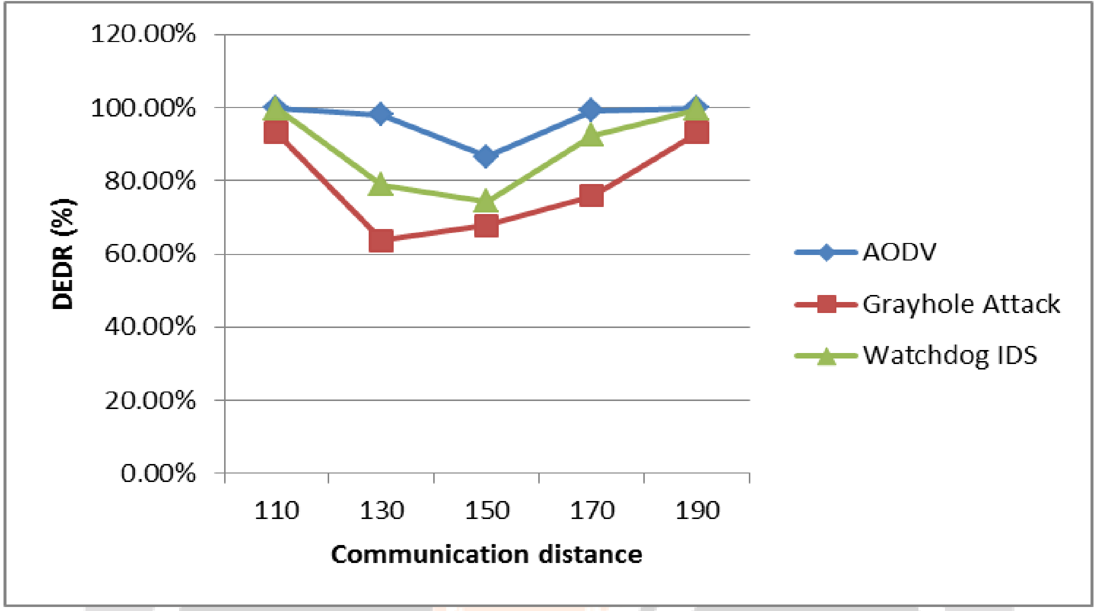

Figure 3: Distinct-Event Delivery ratio versus Communication distance.

- *Distinct-event delivery ratio*

Fig. 3 shows the measured distinct event delivery ratio for AODV routing protocol under gray hole attack and its proposed prevention mechanism namely watchdog intruder detection scheme in terms of the measured distinct event delivery ratio of sensors nodes when communication distance is varied between 110 to 190 meters. The results show that the measured distinct event delivery ratio of watchdog mechanism is higher as compare to the measured distinct event delivery ratio of gray hole attack when the communication distance is higher

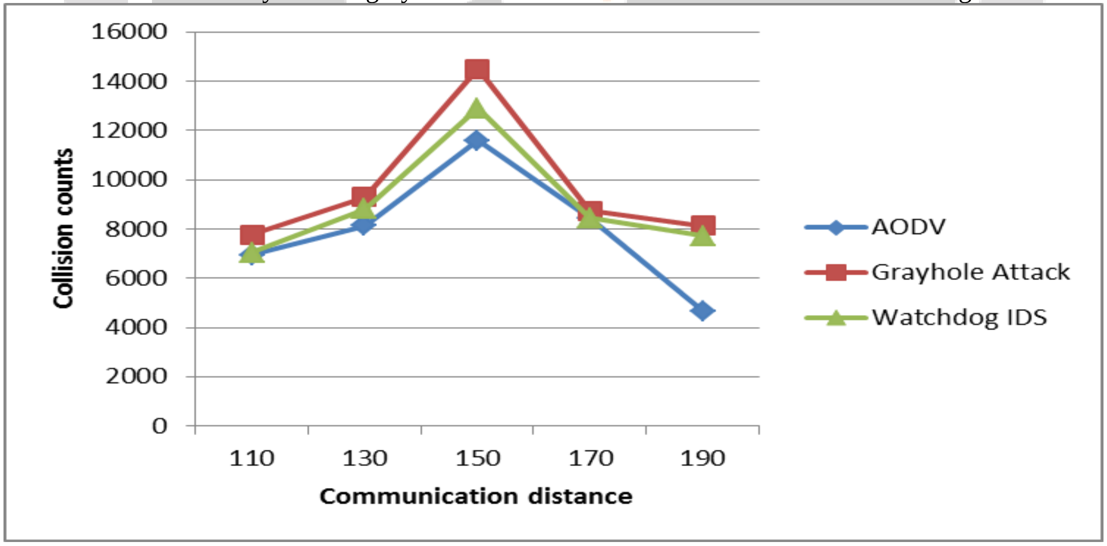

Figure 4: Collision count versus Communication distance.

.

- **Collision count**

Fig. 4, shows the measured collision counts for different commination distance under AODV along with gray hole and its prevention mechansim. The results show that the measured collisions of gray hole is higher as compare to the collisions of watchdog IDS system implemented over AODV routing protocol.

4. CONCLUSIONS

A basic technique to protect data is encryption; but, due to resource constraints, achieving necessary key agreement for encryption is not easy. Cryptographic and authentication protocols have been proposed to protect these networks from outsider intrusions but fail to protect them from the insider ones. most of them focus on the anomaly detection in general assuming that the intrusion is kind of anomalies. Watchdog mechanism proposed in is a monitoring method used for wireless sensor networks, and is the basis of many misbehaviour detection algorithms and trust or reputation systems. Simulation Results show the difference between the amount of sensor network life time and its performance affected by gray hole attack and how much its effect reduced using modified intruder detection scheme namely watchdog AODV against gray hole attack using different performance metrics namely remaining energy, Average end to end delay, Distinct event delivery ratio, and number of collisions. Simulation results depicts that proposed watchdog intruder detection scheme against Gray hole attack works for secure communication, data aggregation and intrusion over wireless sensor network.

REFERENCES

[1]. S. Dai, X. Jing, L. Li, " Research and Analysis on Routing Protocols for wireless sensor networks," In IEEE, Vol. 1, pp. 407-411, May 2005.

[2] H. Pham and S. Jha, "Addressing Mobility in Wireless Sensor Media Access Protocol," in Proc. IEEE Intelligent Sensors, Sensor Networks and Information Processing Conference, Melbourne, 2004, pp.113-115.

[3] M.Ali and Z.A.Uzmi, "Medium access control with mobility-adaptive mechanisms for wireless sensor networks," *Int. J. Sensor Networks*, 2006, Vol. 1,Nos. 3/4, pp.134–142.

[4] K. Akkaya , M. Younis , "A Survey on Routing Protocols for Wireless Sensor Networks," In Elsevier, Vol. 3, pp. 329-345, May 2005.

[5] Onkar V.Chandure, V.T.Gaikwad, "Detection & Prevention of Gray Hole Attack in Mobile Ad-Hoc Network using AODV Routing Protocol" International Journal of Computer Applications, *Volume 41, issue 5 , March 2012.*

[6] Chetan S. Dhamande, H. R. Deshmukh, "A Efficient Way To Minimize the Impact of Gray Hole Attack in Adhoc Network" International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 2, February 2012.

[7] Tarun Varshney, Tushar Sharmaa, Pankaj Sharma, "Implementation of Watchdog Protocol with AODV in Mobile Ad Hoc Network" *Fourth International Conference on Communication Systems and Network Technologies, IEEE, Oct. 2014, pp 217-221.*

[8] Adnan Ahmed, Kamalrulnizam Abu Bakar and Muhammad Ibrahim Channa, "Performance Analysis of Adhoc On Demand Distance Vector Protocol with Blackhole Attack in WSN" Journal of Computer Science, Science Publications, ISSN: 1549-3636, 2014, pp. 1466-1472.

[9] Smita Karmakar and Alak Roy, "Holes Detection in Wireless Sensor Networks: A Survey" Modern Education and Computer Science, MECS, 2014, pp. 24-30.

[10] Benamar Kadri, Djilalli Moussaoui, Mohammed Feham and Abdellah Mhammed, "An Efficient Key Management Scheme for Hierarchical Wireless Sensor Networks" Wireless Sensor Network,Scientifi research, June 2012, pp. 155-161