ANALYSIS OF PACKET DELAY ON ROUTING PROTOCOL IN WIRELESS SENSOR NETWORKS

S.MOHANAPRIYA
Asst.professor
Department of Computer Science
Padmavani Arts & Science College for Women
Salem-11

A.AKILANDESWARI
Asst.professor
Department of Computer Science
Padmavani Arts & Science College for Women
Salem-11

M.NITHYA
Asst.professor
Department of Computer Science
Padmavani Arts & Science College for Women
Salem-11

Abstract

Wireless sensor network (WSN) is a network of devices that can communicate information from one device to another device through wireless links. It consists of base stations along with numbers of nodes. Packet delay is a major issue during data transmission, which is caused by link error. In conventional methods, the packet delay affects the network performance. Packet delay is due to regular link errors or combined with link error and malicious drop. To overcome these problems we have proposed a novel method HLA based on the routing scheme with auto correlation. Here, the proposed technique will be implemented in DSR (Dynamic Source Routing) protocol. During the data transmission, the packet delay information described by our technique. Our proposed technique comparable with other routing protocol using the NS2 simulator.

Keywords: WSN, HLA, DSR, Packet Delay, NS

I. INTRODUCTION

Wireless sensor networks are low powered devices used in a variety of monitoring applications such as healthcare environment or structural health monitoring as well as military surveillance. As most of these applications require in field deployment where human access is seldom possible, reducing the energy consumption of the network is of high importance. To address this issue a considerable number of protocols for WSNs has been developed with the purpose of extending the network Lifetime.

The existing model described to packet delay in implementing various process steps. The model is used to make the implement of correlation process. The node activities easily modified by performing simple and efficient process. It should be processed by identifying packet delay framework of the system. The data is stored in simple and efficient model. The user is responsible to maintain the system and transmit the data from the insecure network. The packet delay is easily solved by the mechanism overcoming by the system representation. The previous AODV protocol is not useful for processing data in the complex netw ork.

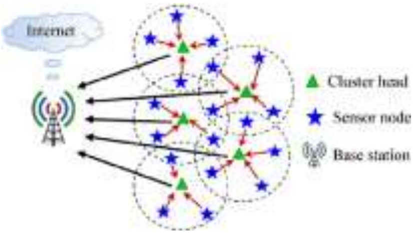

Figure 1. Wireless Sensor Network

A Mobile Ad hoc NETwork is a kind of wireless ad-hoc network, and is a self configuring network of mobile routers connected by wireless links. Mobile Ad-Hoc Network (MANET) is a wireless network without infrastructure. Self configurability and easy deployment feature of the MANET resulted in numerous applications in this modern era. Efficient routing protocols will make MANETs reliable. MANET problems are not easy to be solved.

MANETs face various security threats in which the traffic is redirected to such a node that actually does not exist in the network. Black Hole attack disturbs the routing protocol by misleading other nodes about the routing information. In the Black Hole attack a malicious node uses its routing protocol in order to induce itself for having the shortest path to the destination node or to the packet it wants to interrupt. Another problem is “sinkhole problem” that means when the user assigns unique information, the node that has presented the information is trustworthy node”[1]. These problems solved by the proposed method.

II.RELATED WORKS

In wireless sensor networks, many works have been done to improve the performance of networks. There is a lot of related work about the wireless sensor network.

Routing protocols play an important role in the energy efficiency of WSNs as they contribute to the reduction of energy consumption and latency and they provide high data throughput and quality of service of the sensor network. In order to obtain efficient communication paths, routing protocols take into consideration one or more of several metrics which are further described [2].

Kris Gaj expands the Cryptography concepts such as confidentiality, integrity, and authentication, are required in many of the billions of small devices constituting the “Internet of Things”. Such devices could include cyber-physical sensors and actuators, wireless sensors, biometric devices, driverless cars [3].

Churn-Pong Lai and Cunsheng Ding says the concept of threshold scheme that can be useful in Cryptographic keys. We can encrypt data to protect data. It is highly unsafe in a single inconvenience can make the information inaccessible [4].

The range of MANET routing protocols available and discuss the functionalities of several ranging from early protocols such as DSDV to more advanced such as MAODV, our protocol study focuses upon works by Perkins in developing and improving MANET routing. A range of literature relating to the field of MANET routing was identified and reviewed, we also reviewed literature on the topic of securing AODV based MANETs as this may be the most popular MANET protocol. [5]

Airborne network is an evolving field in the wireless networks. Airborne network is an efficient routing protocol and it is suitable for larger size network. It is based on performance, routing model, network structure and methodology. Performance of routing protocol is tested by a simulator. Performance like packet delivery ratio and time is varied due to other nodes. These parameters are considered in evaluating routing protocol. The method used in the AeroRP, similar to the discovery of neighbors is varied for different protocol [6].

Routing protocols used in mobile ad-hoc networks. A collection of nodes is called as networks which are connected dynamically without using any infrastructure. Various types of routing protocols have been implemented such as OLSR, DSR, AODV, BATMAN etc. The comparison is based on relative DYMO, OLSR and DSR protocols. These protocols are implemented in a different simulation environment. The proposed work has been selected a suitable routing protocol. These three protocols are simulated in a sample network using a set of parameters [7].

Using directional antennas in wireless sensor networks. We have found that using directional antennas not only can increase the throughput capacity but also can decrease the delay by reducing the number of hops. We also construct a time-division multi-access (TDMA) scheme to achieve this. Compared with omnidirectional antennas, directional antennas can reduce the interference and lead to the improvement of the network capacity. Furthermore, directional antennas can extend the transmission range, which leads to fewer hops and the lower multi-hop routing delay [8].

Mobile entities are also called as MULEs which elect to choose up data from sensors in close range, buffer it and drop it at wired access points. The MDC tour is molded as a TSP and the mobile agent periodically traverses the network to collect the data and dump it in the sink. A similar architecture was proposed in, where the network is divided into clusters by a k-means clustering based mechanism and a cluster head is placed in each cluster [9][10].

A transport handles the congestion and reliability. In wireless sensor network (WSN), applications require a congestion control mechanism to regulate the large amount of traffic to inject within WSN to avoid packet loss and to assurance E2E reliable packet delivery[11]. WSN researchers thus argue the presence of a transport layer for WSN similar to the Internet. Because of the resource constraint nature of sensor devices, however, researchers admit that an Internet-scale transport layer will indeed be a matter of challenge [12][13].

III. PROBLEM IDENTIFICATION

In the existing model for maintaining a simple processing capability, the data can be securely sent from one source to another. The basic data transmission is simple, but the security is still inadequacy. The existing model is only supported to find the unsafe node in the network. The involvement of the system is to find the malicious node in a simple and efficient way. Thus the data can be easily sent to one process to another. The main objective of processing is to detect the node. The processing of maintenance is to follow the basic maintenances that are provided.
The system is maintained to form the systematic model. The formation of the model is to be maintained under the scheme through which it can be formed. The systematic development of the process can be used under different sources to be solved.

1) Credit system:
In this type of system, a node receives credit by sending packets for other nodes. These credits are used by nodes to send its own packets. If a malicious node is continuously dropping the packets, then it will lose credits and it cannot send its own traffic.

2) Reputation system:
Here the system depends on neighbor nodes to identify the malicious node. A node which drops most of the packets will get a bad reputation by its neighbor node. This information is passed to all the nodes in the network and is used to select routes for the next packet transmission. A high packet dropping node is eliminated from the roots.

3) End-to-end or hop-to-hop acknowledgement:
Here end-to-end or hop-to-hop acknowledgements are used to find the hops where packet loss is present. A hop that high packet dropping rate is eliminated from the route.

4) Usage of cryptographic primitive methods:
This type is used to construct the proofs for the forwarding of receiving a packet at each node

Architecture of Problem Identification

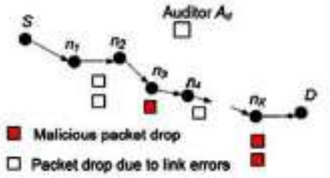

Figure 2. Architecture of Problem Identification

Consider a multi-hop network, which is having an arbitrary path PSD as shown in above figure. The source node sends the packets through intermediate nodes to the destination node. In each hop, the sending node is called as an upstream node of a receiving node. The packets are transmitted from source to destination and a bitmap is obtained for each node as (a1, a2.... am) where a=0 or 1. If the packet is successfully transmitted, then a=1 and if the packet is not transmitted the value of age is considered as 0. By using this bitmap we can find the correlation between the lost packets. From this correlation we can find the malicious node.

There is an auditor in the network which is independent. The meaning of independent is that it is not related to any of the nodes in the network and it doesn't know about the secrets associated with the nodes. Here auditor is capable of detecting attacker's nose when it gets a request from the source. After sending all the packets from source to destination, the destination sends a feedback to source about the route, i.e. whether the route is under attack or not by considering some parameters. After getting feedback, if the route seems to be under attack, then the source will send the attack detection request (ADR) to the auditor. Now the auditor starts investigation to find the malicious node. The auditor requests certain information from the intermediate nodes. Here normal nodes reply with the correct information and the malicious node try to cheat. Here

each and every node must reply to the audit or request otherwise the node is considered to be misbehaving.

Disadvantage

The main drawback found in the existing model is the Link error finding. This drawback is overcome by the proposed model. A scheme called elegant routing is used to overcome the computation and communication overhead in the network.

IV. PROPOSED METHOD

In this work, the existing disadvantage is to overcome by finding the packet delay due to the Link Error. This can be done by implementing the robust routing scheme that is better than the existing AODV protocol. The protocol modification is done by replacing AODV with DSR routing work. Another use of the proposed work is used to maintain truthful detection by implementing HLA. Thus the packet loss detection is simple. But the link or route implementation is based on the DSR routing concept. Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of mobile nodes. DSR allows the network to be completely self-organizing and self-configuring, without the need for any existing network infrastructure or administration. DSR has been implemented by numerous groups, and deployed on several test beds.

The security algorithm used in this work is the RSA cryptographic Algorithm. This algorithm is simple and robust to overcome the packet dropping attack in the network. Thus, this should be used to maintain under the simple and efficient scheme.

Proposed Architecture

To simplify the systematic update of the meaningful environment through which it can be used. The HLA mechanism is introduced to process the simple and the DSR routing protocol. The purpose of HLA is to send a message to all nodes and wait for the ACK from all nodes. Only some nodes have sent an ACK to HLA, and these nodes are identified as trustworthy. Now the nodes can transfer the packets by finding the shortest path in the trustworthy node list. Another use of HLA is to monitor all the nodes, if the destination nodes don't receive the packet, it sends an ACK to HLA. Now HLA starts monitoring and finds the malicious node which holds the packet or if any link error occurs.

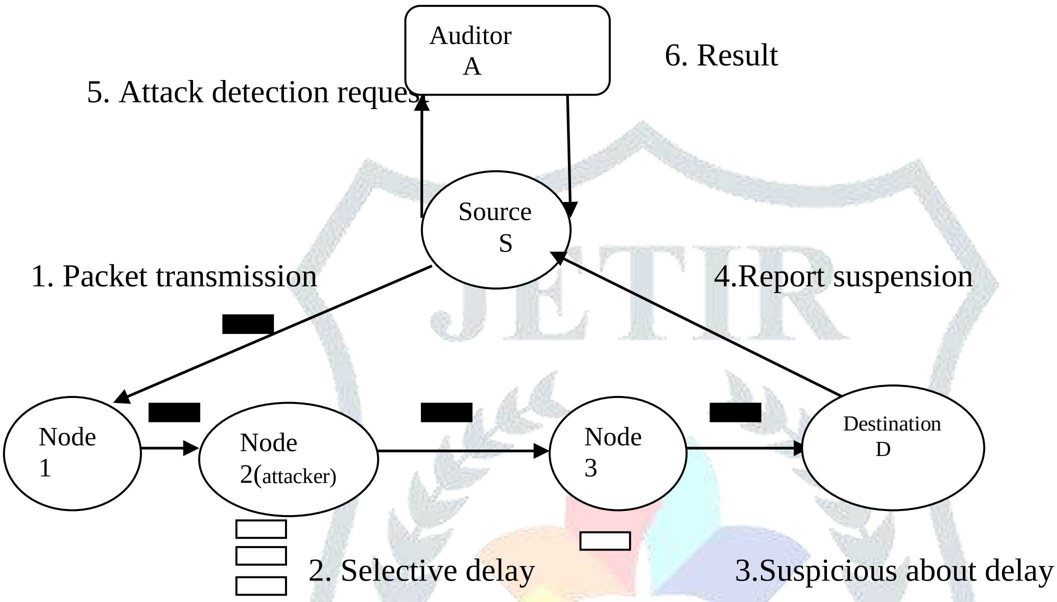

Figure 3.Architecture of Proposed Model

DYNAMIC SOURCE ROUTING PROTOCOL

The protocol is composed of the two main mechanisms of Route Discovery and Route Maintenance, which work together to allow nodes to discover and maintain routes to arbitrary destinations in the ad hoc network. All aspects of the protocol operate entirely on-demand, allowing the routing packet overhead of DSR to scale automatically to only that needed to react to changes in the routes currently in use.

The protocol allows multiple routes to any destination and allows each sender to select and control the routes used in routing its packets, for example for use in load balancing or for increased robustness. Other advantages of the DSR protocol include easily guaranteed loop-free routing, support for use in networks containing unidirectional links, use of only soft state in routing, and very rapid recovery when routes in the network change. The DSR protocol is designed mainly for mobile ad hoc networks of up to about two hundred nodes, and is designed to work well with even very high rates of mobility.

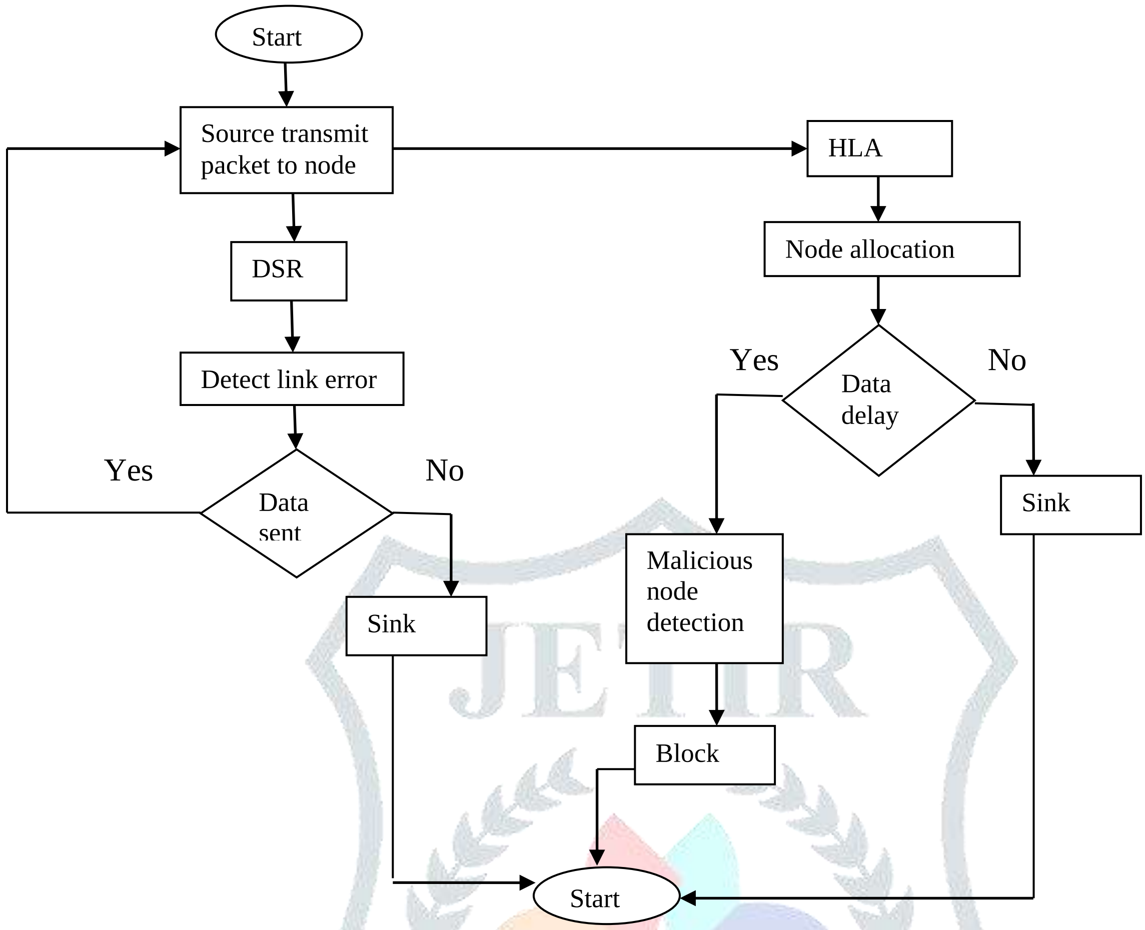

Figure 4.Flowchart for Packet Delay

Here the data transmission is started in a source area. Then the packet formation is used. And then the DSR process has taken place by building the process in a various formats to make the data can be used to process for the simple environment. This can be maintained under the source that should be used for various other hops to transmit the data. The proposed model successfully overcomes the link error. Then the next process is the data transmission to the sink. If the data is not properly transmitted the next process is to detect malicious node, and this process is done with the help of the HLA. Then the data are transmitted to the sink node.

Algorithm Used for Security

The RSA algorithm used for data privacy in this research work. The algorithm has the following steps: key generation, encryption, decryption.

Key generation:

1. Select a random prime numbers p and q, and check that p != q
2. Compute modulus n = pq
3. Compute phi, φ= (p - 1) (q - 1)
4. Select the public exponent e, 1 < e < φ
   Such that gcd (e, φ) = 15.

Compute private exponent d = e -1modφ
6. The public key is {n, e}, the private key is d

Encryption:

C = me mod n

Decryption:

m = cd mod n

Digital signature: s = H (m) d mod n, Verification: m' = send in, if m' = H (m)signature is correct. H is a publicly known hash function

V.RESULTS AND DISCUSSION

Packet delivery ratio

Table 1. Packet delivery ratio in existing system

Number of packet transmission	Packet delivery ratio in existing system	
	AODV(%)	DSR(%)
10	0.6	0.3
20	0.55	0.3.3
30	0.41	0.2

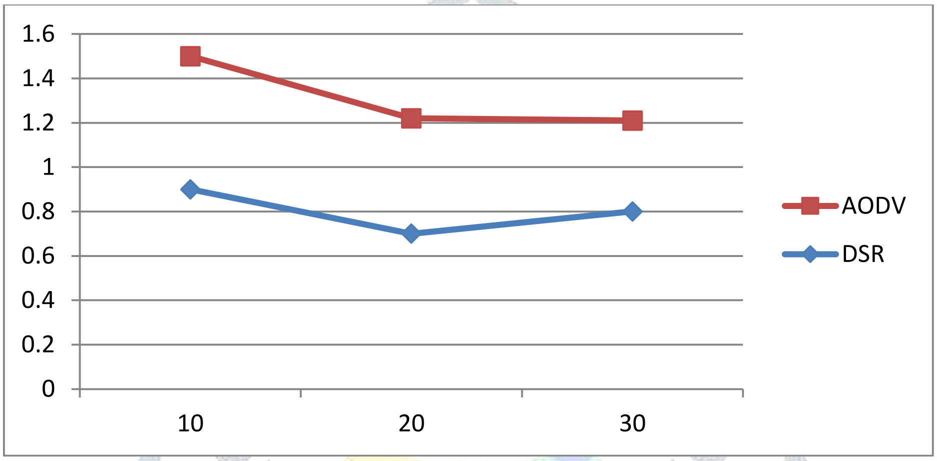

Figure 5. Packet delivery ratio in existing system

Figure 5 and Table 1 describe the packet delivery ratio of existing system. If 10 packets are transmitted using AODV the packet delivery ratio is 0.6% it is higher than DSR because the packet delivery ratio of DSR is 0.3%. So in existing system packet delivery ratio of AODV are higher than DSR. The calculation format can also be required for the above mechanism which are derived below.

1.Throughput

It refers to the number of packets successfully transmitted from source to destination.

Throughput=total No.of packets received/total No.of time

2. Delay

Analysis of average delay refers the process of sending and receiving of packets

Table 2. Packet delivery ratio in proposed system

Number of packet transmission	Packet delivery ratio in proposed system	
	DSR(%)	AODV(%)
10	0.9	0.6
20	0.7	0.52
30	0.8	0.41

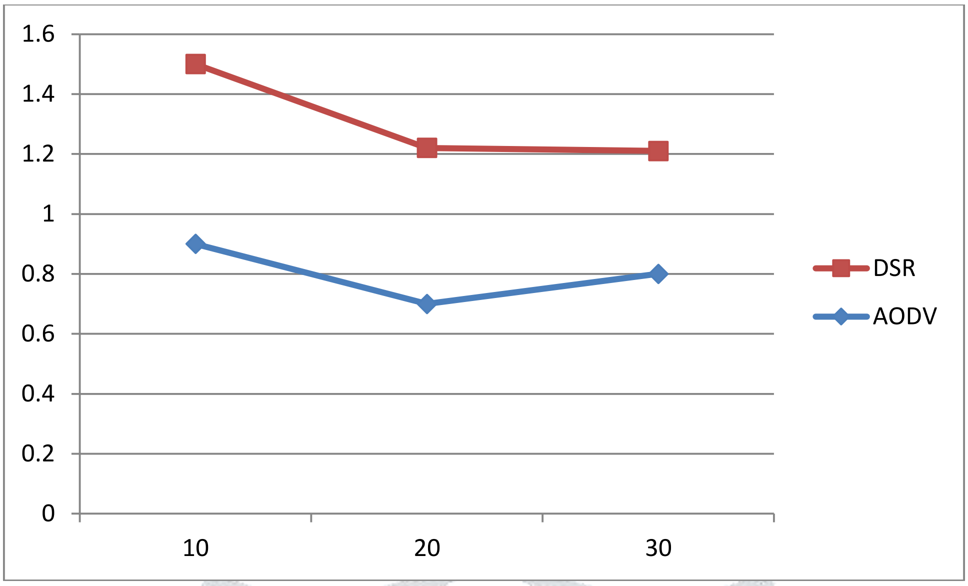

Figure 6. Packet delivery ratio in proposed system

Figure 6 and Table 2 describe the packet delivery ratio of this research work. If 10 packets are transmitted using DSR with auto correlation mechanism, the packet delivery ratio is 0.9% it is higher than AODV because the packet delivery ratio of AODV is 0.7%. Here DSR has highest packet delivery ratio because of using an additional mechanism called auto correlation. So in this research work the packet delivery ratio of DSR is higher than AODV.

VI.CONCLUSION AND FUTURE WORK

Wireless Sensor Network (WSN) suffers from link error and packet delay. The characteristics of routing protocols AODVand DSR are studied and further, we modified the DSR protocol with an auto - correlation mechanism to perform well than the other existing protocols. Implementation of autocorrelation mechanism is DSR will find the shortest path and high speed data transmission can be carried out in the network environment. The anchor node selection is also implemented in the research work. The anchor node is used to detect the packet delay and link error using auto -correlation mechanism. Thus, proposed model performs well than the existing models on the basis of computation time and communication overheads. Further, we compared the performance of proposed OLSR (Auto-correlation mechanism) with the existing protocols such as AODV. Our future work the same algorithm can be implemented with different mobility model and routing protocol.

References

1] H. Deng, W. Li and D. P. Agrawal, Routing security in wireless adhoc networks, IEEE Commun. Mag., 40 (10): 70-75, October 2002

2] R. Draves, J. Padhye, B. Zill, “Comparison of Routing Metrics for Static Multi-Hop Wireless Networks”, In the Special Interest Group on Data Communication Conference, SIGCOMM’04, September 2004

3] Comparing the Cost of Protecting Selected Lightweight Block Ciphers against Differential Power Analysis in Low-Cost FPGAs, 23 April 2018

4] Chun-Pong Lai and Cunsheng Ding “Several Generalizations of Shamir's Secret Sharing Scheme” Vol. 15 No. 2 (2004) 445-458

5] Alex HindsMichael Ngulub, Shaoying Zhu, and Hussain Al-Aqrabi,” A Review of Routing Protocols for Mobile Ad-Hoc NETworks (MANET)” Vol.3, No. 1, February 2013.

6] B. Awerbuch,R.Curtmola,D.Holmer,C.Nita-Rotaru, and H.Rubens, “ODSBR: An on demand secure byzantine resilient routing protocol for wireless ad hoc networks”,ACMTrans.InformSyst.Security,vol.10.no.4,pp.1-35,2008.

7] K.Balakrishnan, J.Dengand, P.K.Varshney, “TWOACK Preventing selfishness in mobile ad hoc networks,” in Proc. IEEEWirelessCommun Network Conf., 2005, pp.2137-2142.

8] Hong-Ning Dai “Throughput and Delay in Wireless Sensor Networks
using Directional Antennas”, The Chinese University of Hong Kong, Hong Kong

9] L. Tong, Q. Zhao, and S. Adireddy, “Sensor networks with mobile agents”, in Proc. IEEE MILCOM, Boston, MA, October 2003.

10] Jayashree C. Pasalkar Vivek S. Deshpande, Dattatary Waghole,” Performance Analysis of Delay in Wireless Sensor Networks”, 2012

[11] TaoShuand Marwan Krunz,“Privacy Preserving and Truthful Detection of Packet Dropping Attacks in Wireless Adhoc Networks”,IEEE Transactions on Mobile Computing, Vol.14,no.4,April 2015.

[12] B.Awerbuch,R.Curtmola,D.Holmer,C.Nita-Rotaru, and H.Rubens, “ODSBR: An on demand secure byzantine resilient routing protocol for wireless ad hoc networks”,ACMTrans.InformSyst.Security,vol.10.no.4,pp.1-35,2008.

[13] Namesh, C., and Dr B. Ramakrishnan. "Analysis of VBF protocol in Underwater Sensor Network for Static and Moving Nodes." International Journal of Computer Networks and Applications 2.1 (2015): 20-26..