ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 5, May 2016

Securing Wireless Sensor Networks from Selective Forwarding Attack

Rachana Srivastava[1], Inderjeet Yadav [2]

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & NGF College of Engineering &Technology
Palwal, Haryana, India

***Abstract*— Security is the serious subject in wireless sensor networks. Thus, WSNs are vulnerable to various kinds of security attacks. One cause to attack sensor networks is the restricted capacity of sensor nodes. The security attacks could influence the most important applications in WSNs field i.e. traffic monitor, military surveillance and healthcare. Hence, there are several kinds of detection mechanisms against security attacks in WSNs on the network layer. Also, there are severe restraints on sensor nodes i.e. energy efficiency, reliability and scalability, which influence the WSNs security. However, the sensor nodes have restricted abilities for most of these restraints, a selective forwarding attack is complicated to determine in the networks. Harmful nodes in the selective forwarding attack, perform as normal nodes. Since, it tries to detect the sensitive messages and discard them before forwarding the packet to other nodes. For keeping this kind of attacks farther from networks, we introduce a multi layers technique (SFD) that preserves the safety of data transmission among sensor nodes while finding the selective forwarding attack. Moreover, the technique involves energy efficiency, reliability and scalability.**

Keywords*— Wireless Sensor Networks (WSNs) and Selective Forwarding Attacks.

I. INTRODUCTION

Sensor networks collect data that is essential to involve in smart networks atmosphere. For example, these atmospheres involve transportation system, home, healthcare, military and buildings. The study WSN is an interested topic in computer science and engineering. WSNs have an influence on economics, and impact industrial industry. It consists multiple sensors, in fact these sensors interact with a large no. of small nodes through radio connections. Sensor networks have a source and a BS. WSNs maintain thousands of sensor nodes. A sensor contains four basic units, sensing unit: transceiver, processing and power [1]. Currently several distributed sensor networks can be spread, and have a self-configuring capability. Within the computation capability of WSNs techniques development, the mechanism must ensure that sensor nodes are not overloaded with too various complex functions.

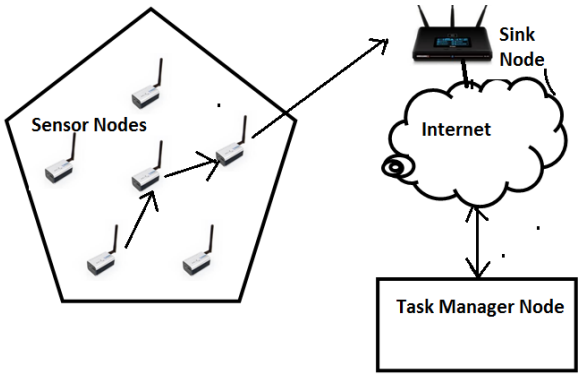

Figure 1: Wireless Sensor Networks

The wireless sensor networks security has been extensively inquired over the last few years. WSNs are vulnerable to several kinds of attacks because they support as an open network with the restricted resources of nodes. Thus, the obstructions of protecting a WSN are the main drawback for all devices. The most traditional attacks to the wireless sensor networks security involve node compromised, eavesdropping, disrupt, modify or inject harmful packets, compromised privacy and DoS attacks [2]. Networks have various applications. Thus, applications contain various levels of tracking, monitoring, tracking and controlling. A collection of applications are used for particular aims. In military applications, sensor nodes involve battlefield surveillance, monitoring and object tracking. The battlefield monitors used in military operations have motivated the growth of WSNs. In medical applications, sensors support in patient diagnosis and monitoring. Here, most applications are spread to monitor a region and then react when a sensitive factor is stored [3]. In general, sensor networks have

strong applications in several industrial i.e. factory instrumentation, environmental monitoring and inventory tracking.

II. SECURITY CONCERN IN WSN

A. *Data Confidentiality:* Confidentiality is an acceptance of authenticated access to information communicated from a trusted sender to a trusted recipient. A sensor network must not disclose sensor readings to its neighbouring nodes. Highly sensitive data is sometimes forwarded through several nodes before arriving the final node. For protected communication, encryption is employed. Data is encrypted with a secret key that only authenticated subscribers have. Public sensor information should also be encrypted to some degree to secure against traffic analysis attacks. [11]

B. *Data Integrity:* Provision of data confidentiality stops the information outflow, but it is not useful against adding of data in the actual message by attacker. Data integrity requires to be confirmed in sensor networks, which concentrates that the obtained data has not been modified with and that new data has not been joined to the actual packet contents. Data integrity can be offered by Message Authentication Code (MAC) [13].

C. *Data Authentication:* An adversary is not only restricted to temper the data packet but it can modify the complete packet stream by adding additional packets. So the recipient requires assuring that the data utilized in any decision-making method comes from the authenticated source. Data authenticity is an assurance of the communicating nodes identities. Nodes participating in the communication must be capable of identifying and rejecting the information from illegal nodes. Authentication is needed for several administrative tasks [11].

D. *Data Freshness:* Data freshness assures that the data communicated is latest and no prior messages have been replaced by an antagonist. Data freshness is categorized into two types depending on the message ordering [9]; strong and weak freshness. Weak freshness offers only partial message ordering but provides no information regarded to the latency and delay of the message. Strong freshness on the other side, provides entire request-response pair and permits the delay estimation. Sensor measurements need weak freshness, while strong freshness is required for time synchronization within the network. For confirming the packet freshness, a timestamp can be associated to it. Destination node can compare the timestamp with its own time clock and examines whether the packet is valid or not.

E. *Availability:* Availability is an insurance of the endowment to indulge required facilities as they are planned earlier. It confirms that the network services are viable even in the denial of service attacks subsistence. For making data existence, security protocol should pursue less energy and storage, which can be aimed by the reutilization of code and making confirm that there is little increase in communication because of the services of security protocols. Central point technique should also be neglected as single point failure will be proposed because of this in a network that threatens the existence.

F. *Self Organization*

A normal WSN may have thousands of nodes satisfying several operations, installed at various locations. Sensor networks are also ad hoc networks, having the same extensibility and flexibility. Sensor networks require each sensor node to be ductile and independent enough to be self-healing and self-organizing according to various situations [13].

G. *Time Synchronization*

Most sensor network applications based upon some form of time synchronization. For skimping power, an individual sensor's radio may be switched off for some time. Furthermore, sensors may need to compute the packet end-to-end delay as it travels between two pair wise sensors [14].

H. *Secure Localization*

WSN makes utilization of geological based information for nodes recognition, or for accessing whether the sensors correspond to the network or not. Many attacks work by investigating the nodes location. Attacker may examine the packets header and protocol layer data for this objective. This builds the protected localization a significant characteristic that must be fulfilled during our security protocol implementation [14].

I. *Flexibility:* Sensor networks will be utilized in vigorous arena scenarios where environmental conditions, mission and hazards may change quickly. Changing mission objectives may need sensors to be removed from or injected to a settled sensor node. Furthermore, two or more sensor networks may be combined into one, or a single network may be classified in two. Key establishment protocols must be ductile enough to render keying for all potential scenarios a sensor network may detect.

J. *Robustness and Survivability:* The sensor network should be robust throughout several security attacks and if an attack conquers, its effect should be decreased. The covenant of a single node must not damage the whole network security.

III. RELATED WORKS

Gagandeep Singh et. al [2]; evaluating wireless sensor network on quality of services using Mobile

sink nodes. For the simulation purpose authors has taken OPNET as simulation tool. In their work author purpose COMN2 a scalable and distributed approach for congestion control and network recovery from node failures in WSN. After the simulation result author conclude that mobile communication shows better results in term of throughput, has less response time, traffic sends and traffic receives is also high in case of mobile sink scheme as compare to multi hop with congestion scheme.

Er Gurjot singh et. al [3]; enhancing quality of service in WSN by using symmetric key cryptographic schemes. For the simulation purpose author has taken QUALNET4.5.1 network simulator tool that is used to evaluate the performance of different cryptographic schemes. After the simulation result author concludes that symmetric key cryptography schemes require less storage space, less power and require less time for processing, and less impact on the quality of services of WSN.

Yi cheng et. al [4]; In this paper authors using low energy consumption method for energy efficient session key management in WSN. In their work author purpose a mechanism that based on symmetric keys. For their work author has taken 1000 no. of nodes,100 cluster head and 200second simulation time .after the simulation result they found that the proposed mechanism improve routing overhead & security.

Surinderjit kaur et. al [5]; here author purposed a secure symmetric key based mechanism for synchronization purpose. In their technique they also describe Blowfish algorithm. For the simulation purpose author has taken three performance matrices such as delay, throughput and network load. After the simulation result derived from simulation a comparison is shown that describe the proposed mechanism improve throughput and network load. At last author conclude that a clustering technique is much better than other technique for energy efficiency.

Yu and Xiao [6] introduced a technique depending on lightweight security to determine a selective forwarding attack in the sensor networks environment. The technique used a multi-hop acknowledgment to set up alarms by getting replies from the nodes that are positioned in the middle of paths. Authors considered the technique could detect harmful sensor nodes. The objective of the detection attack is to forward an alarm when a dangerous node is detected, which shows a selective forwarding attack. The authors observed that the detection accuracy of their technique exceeds 95% with an error rate of 15%. Yu and Xiao used two detection mechanisms in the strategy: a downstream process (the direction on the way to
the BS) and an upstream process (the direction on the way to the source node). In the upstream process, a report packet is generated and forwarded to the BS hop by hop when nodes find a harmful node. Thus, the BS would obtain the alarm packet and send various hops that are created by the node. An alert packet and acknowledgement packet will drain the energy at the time of detection.

The detection of malicious nodes is informed through an intermediary node. First, Xiao, Yu, and Gao [7] introduced a checkpoint-based method. In this mechanism, a node is randomly chosen as the checkpoint to forward an acknowledgement message for determining the antagonist. It is a technique utilized to detect malicious nodes in a selective forwarding attack. They have tried to enhance the mechanism by determining an abnormal packet in sensor networks. They considered that any compromised nodes could not generate alert packets with the objective of maliciously prosecuting other nodes. After gathering proofs to detect whether the node is a harmful node, the source nodes identify the position of the malicious node according to the location. Since, it is no confirm for reliable transmission of messages even though the antagonist is located by acknowledgement.

Tran Hoang and Eui-Nam [8] introduced a technique against selective forwarding attacks that contains a lightweight detection technique. The detection is a centralized cluster, which used the two-hop neighborhood node information and over listening mechanism. It is based on the broadcast behavior of sensor interaction and the high density of sensors. Every sensor node is offered with a detection module that is built on an application layer. Sensor node adjusts routing rules and two-hop neighbor knowledge to create an alert packet. Hoang and Nam proposed that the two routing rules build the monitoring system more appropriate. Therefore, the first rule is to detect if the destination node sends the packet along the route to the sink. It creates an alert packet with the malicious factor α to the source/sender node. The second rule governs that the monitor node waits and determines the packet that was already sent along the path to the sink. It tests the two-hop neighbor knowledge to assess whether the destination node is on the right path to the sink. If not, it creates an alert packet with the malicious factor β to the source/sender node.

The detection module is responsible for passively determining a selective forwarding attack in its neighboring sensor node. The malicious counter is described as the threshold of abnormal activity in a

sensor node, which could not ignored. When the malicious counter exceeded the threshold X, it revoked the dangerous node from its neighboring list. The authors have considered that the neighboring node should be identified. The neighboring node must be protected and authorized in the deployment time. The network has a fixed configuration and utilizes key management to prevent any outside attacks. The choice of one kind of network configuration prevents the mechanism from working with other configurations.

IV. SELECTIVE FORWARDING ATTACKS

A network layer in WSNs is proposed to various kinds of attacks. Moreover, a sensor node may achieve benefits of multi-hop by simply denying to route packets. Thus, it could be carried out all the time with the net result. If a neighboring node marks a route via the atacker node, then it will be unable to alter messages [4]. There are varieties of attacks targeting the network layer. The intruder can attack the routing protocol by inserting the path between the source node and the base station.

In WSNs, there are two kinds of attacks: insider and outsider attacks. One of the insider attacks is known as a selective forwarding attack. In selective forwarding attack, the antagonists are capable to generate routing loops that repel or attract network traffic. Also, they can increase or decrease source routers, create wrong messages, and try to discard the important messages. The selective forwarding attack is complicated to detect specifically, when compromised nodes discard packets selectively. The discarded packets come from one node or a collection of nodes. A harmful node denies to send the messages or discards packets randomly. Therefore, the base station would not obtain the whole messages [5,6].

V. ECC-BASED KEY MANAGEMENT SCHEME

5.1 Introduction: Most available key management techniques try to set up shared keys for all pairs of neighboring sensors, no matter whether these nodes interact with each other or not, and this leads large overhead. This technique offers important decrement in communication overhead, energy consumption and storage space as compared to other key management technique. It obtains important storage saving by using 1) the fact that most sensor nodes only interact with a small portion of their neighboring nodes; 2) an effective public-key cryptography.

5.2 Key Generation Using Elliptic Curve: Select an Elliptic Curve E over finite field. Select a Prime field FP, which contains finite no. of elements between 0 to P-1. The Elliptic Curve over a finite field FP is the collection of all (x,y)(x,y ∈ Fp) that meets the following equation:

$Y2 \bmod P = X3 + aX + b \bmod P$ where a,b,Fp and $4a3+27b2 \bmod P \neq 0$.

If a point is on Elliptic Curve G(XG ,YG) ,then there is least positive integer „n‟ such that nG=O, where “O” is Point of infinity and Integer „n‟ is known as the order of Point G. A scalar K is selected for Point multiplication in b/w 0 and n-1.

The Public Key “Q” is made by following equation:

Q=KG,

where „K‟ is Discrete Logarithm of Q to the base P.

The *elliptic curve discrete logarithm problem (ECDLP) is the following:*

provided an elliptic curve E described over Fq, a point P∈ E (Fq) of order n, and a point Q=E(Fq), compute the integer l, $0 \leq l \leq n - 1$, such that Q = lP, given that such an integer available.

Point Multiplication

In point multiplication a point „G‟ on the elliptic curve is multiplied with a scalar k utilizing elliptic curve equation to get another point Q on the similar elliptic curve.

i.e. Q= kG

Point multiplication is obtained by two basic elliptic curve operations:

Point addition, adding two points K and J to get another point L

Such that L = J + K.

Point doubling, adding a point J to itself to get another point L

Such that L = 2J

VI. PROPOSED SYSTEM

In WSN, various nodes transfer sensor readings to the BS to process data. Military bases might detect the significance of utilizing sensor networks for exploring enemy forces. Sensor nodes have restricted sensing and computation. Also, nodes have interaction capability. Sensor readings gather data when it finds unusual activities of enemy forces i.e. war tanks and warplanes movement in battlefields. Data will be forwarded to the BS via routers. As depicted in Fig 1, the intruder compromised the nodes by networks attacking. In military applications, selective forwarding attacks damage the transmission packets between the source node and BS, and sometimes among the sensor nodes. Malicious nodes deny transferring a whole packet. It discards the sensitive information and then sends the rest packet. Moreover, physical attacks frequently happen in WSNs because it is easy for antagonists to execute them.

Our technique detects a protected route at the time of data transmission. In this part, we propose our considerations and detection technique. Sensor networks are vulnerable to various kinds of attacks. The harmful node tries to build some obstacles happen during transferring packets within the networks. The following obstacles may happen: send message to another path, create false route in the network, and delay the packets transfer among nodes.

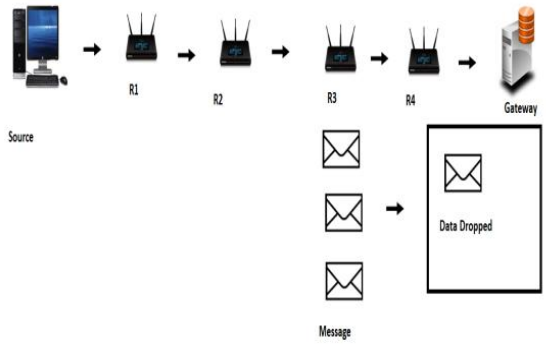

Figure 2: Example of selective forwarding attack

The selective forwarding attack in Fig 2 may occur among sensor nodes. Therefore, node "A" transfers the packets to node "B" and then node "B" ceases sending the packets to node "C". As a result node "B" may send packets to a harmful node. Thus, packets will not reach to the BS.

A. Assumptions: WSN are complex. For creating a simple solution to determine the selective forwarding attack, we have built some considerations for the technique detection within important applications that are vulnerable in networks. These considerations should be acceptable in the sensor networks. First of all, we consider that protected interaction should be part of the networks. Second, dangerous nodes should not discard any packets previous to the selective forwarding attack launching. Third, we consider that the antagonist cannot compromise a sensor node at the time of the deployment. At last, we consider that authentication broadcast protocols were used to every sensor node.

B. Selective Forwarding Detection (SFD) Approach

In WSNs, the rule-based intrusion detection system (IDS) is one of the techniques for security against the security attacks. Rule-based IDS are called signature-based IDS. The network layer in WSNs is threatened through some attacks i.e. a sinkhole attack, a wormhole attack and other kinds of attacks. Our suggestion concentrates on the selective forwarding attack. We plan multi layer method, which involves three security layers shown in Fig 3. The first layer is data receiving. In this layer, the significant information is filtered and buffered. The information involves message fields that are helpful to the rule processing. The second layer is rule processing. In this section, rules must be employed to the buffered data. The message can be denied. In addition, no rules will be used to the message until it fails. The third layer is detection. The detection mechanism saves energy by utilizing low memory and it considers not much time. It selects a protected route to transfer data between the source node and the BS. Moreover, SFD mechanism is energy efficient, reliable and scalable. All these elements are important for the sensor nodes. Our technique considers that the detection accuracy is high, even though the radio condition is worst.

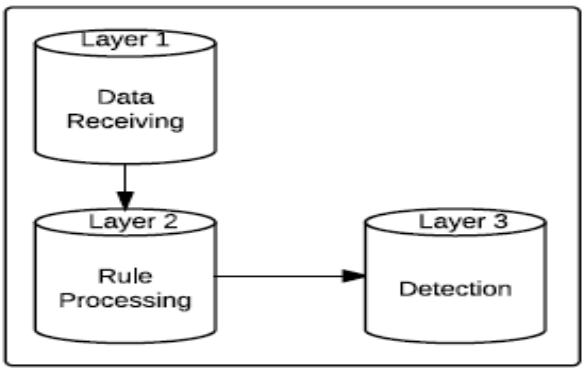

Figure 3: Detection steps in rules based IDS- Redrawn

VII. CONCLUSION

WSNs security has become increasingly concerning. The usage of WSNs is increasingly used in commercial, environmental, military and health applications. Packet security and the transmission period is the basic requirement in WSNs. Selective forwarding attack might be a serious attack on the wireless networks. In this paper, we show a technique that detection selective forwarding attacks over the WSNs. The monitored sensor nodes determine selective forwarding attacks utilizing detector. Our technique is effective to find the attacks. Also, the techniques involve energy efficiency, reliability and scalability.

REFERENCES

[1] Stephan Olariu, "Information assurance in wireless sensor networks", Sensor network research group, Old Dominion University, Wireless Communication and Mobile Computing, Vol. 4,No 6,pp.623-637,2009.

[2] Harpreet Singh, Gurpreet Singh Josan, "Performance Analysis of AODV & DSR Routing Protocols in Wireless Sensor Networks", International Journal of Engineering ,Vol. 2, Issue 5,pp,2212-2216, September- October 2012.

[3], Gurjot singh, Ram singh "A Secure Routing Scheme for Static Wireless Sensor Networks", IEEE Pacific-Asia Workshop on Computational Intelligence and Industrial Application, Vol.2, pp.776-780, 2008

[4] Yi cheng, "Secure Routing in Cluster based Wireless Sensor Networks using Symmetric Cryptography with Session Keys", International Journal of Computer Applications, Vol. 55, Issue. 7, pp.48-52, October 2012

[5] Surinderjit kaur and R.M.S. Parvathi, "Securing Node Capture Attacks for Hierarchical Data Aggregation in Wireless Sensor Networks", International Journal of Engineering Research and Applications (IJERA), Vol. 2, Issue 2, pp.466-474,Mar-Apr 2012.

[6] K.S.Arikumar, K.Thirumoorthy, "Improved User Authentication in Wireless Sensor Networks", 2011 IEEE.

[7] Wassim Drira," A Hybrid Authentication and Key Establishment Scheme for WBAN", IEEE 11th International Conference on Trust, Security and Privacy in Computing and Communications, Vol. 2, No.3, pp.78-83, 2012

[8] Asha Rani Mishra, "Elliptic Curve Cryptography (ECC) for Security in wireless Sensor Network," International Journal of Engineering Research & Technology (IJERT) ,Vol. 1 Issue 3, pp. 2-3,May-2012.

[9] Donnie H. Kim, "Exploring Symmetric Cryptography for Secure Network Reprogramming", International conference on Information, Networking and Automation(ICINA),Kunming, IEEE, pp. 215-218, 2010.

[10] Shohreh Ahvar1, Mehdi Mahdavi, " EEQR: An Energy Efficient Query-Based Routing Protocol for Wireless Sensor Networks", Journal of Advances in Computer Research ,Vol. 2, No. 3, pp. 25-38, August 2011.

[11] Heissenbütte lM., T. Braun, M. Wälchli, and T. Bernoulli, "Optimized stateless broadcasting in wireless multi-hop networks," in proceeding of 4th IEEE international conference on Infocom Barcelona,2006,pp. 234-250.

[12] Sommer, C.; Dietrich, I.; Dressler, F. "Realistic Simulation of Network Protocols in WSN Scenarios" in Proceedings of International Journal of Ad Hoc and Ubiquitous Computing, Vol. 3, 2008, pp. 217-223.

[13] TsengY.C., Y.S. Chen, and J.P. Sheu, "The broadcast storm problem in a Wireless Sensor Networks, " In Proceeding of the 5th ACM/IEEE International Conference on Mobile Computing and Networking, NY, USA,1999, pp. 51-162.

[14] KorkmazG., E. Ekici, F. Ozgüner, and U. Ozgüner, "Urban multi-hop broadcast protocolforWireless Sensor Networks," In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks, NY, USA, 2004,pp. 76-85.

[15] Rajive Bagrodia, Richard Meyer, Mineo Takai, Yu an Chen, Xiang Zeng, Jay Martin, andHa Yoon Song. "A parallel simulation environment for complex systems"in Proceedings of the 1st ACM international workshop on ad hoc networks; 2004; Pages: 66 – 75.

[16] v Brian D. Noble, Jungkeun Yoon ,Mingyan Liu, Minkyong Kim, "Building realisticmobility models in Wireless Sensor Networks", in Proceeding of the ACM International Conference On Mobile Systems, Applications And Services, pp. 177-190, 2006.

[17] Fan Li and Yu Wang; " Survey of Routing in Wireless Sensor Networks",in Proceedings ofIEEE Wireless Sensor Networks Technology Magazine, Volume 2, Issue 2, June 2007; pp. 12-22.

[18] Jahanzeb Farooq, Bilal Rauf "Implementation and Evaluation of IEEE 802.11e WirelessLAN in GloMoSim" In Proceeding of the 1st ACM International Workshop on Ad Hoc Networks, NY, USA, 2004,pp. 76-85.

[19] Yue Liu, Jun Bi, Ju Yang; "Research onWireless Sensor Networks"in Proceedings of Chinese Control and Decision Conference (CCDC), 2009, pp.4430 – 4435

[20] Abedi, O.; Berangi, R.; Azgomi, M.A., "Improving Route Stability and Overhead on AODV Routing Protocol and Make it Usable forWireless Sensor Networks," in Proceedings of 29th IEEE International Conference onWireless Sensor Networks,June 2009, pp.464,467.

[21] Chowdhury, S.I.; Won-Il Lee; Youn-Sang Choi; Guen-Young Kee; Jae-Young Pyun, "Performance evaluation of reactive routing protocols inWireless Sensor Networks," in proceeding of Communications (APCC), 2011 17th Asia-Pacific Conference onad hoc networks ,2011, pp.559,564.

[22] Sun Xi; Xia-Miao Li, "Study of the Feasibility of Wireless Sensor Networks and its Routing Protocols," in proceeding of Wireless Communications, Networking and Mobile Computing, 2008. 4th International Conference on ad hoc networks, 2008, pp.1-4.

[23] Vinod Namboodiri, Manish Agarwal, Lixin Gao; "A Study on the Feasibility of Mobile Gateways for Wireless Sensor Networks", in proceeding of Wireless Communications Networking and Mobile Computing 6th International Conference on 2010,Sept. 2010, pp.1,4, 23-25.

[24] Siva D., Abu B. Sesay, and Witold A. Krzymie´n, "A Design on Routing Protocol in Sensor Networks Based on Clustering Optimization" In Proceedings of 2nd International Conference on Future Computer and Communication,2010, pp 473-477.

[25] C. Y. Wan, S. B. Eisenman, and A. T. Campbell,, "CODA: Congestion Detection and Avoidance in Sensor Networks," In Proceedings of FirstACM Conference on Embedded Networked Sensor Systems,2003,pp.266-279.

[26] R.U.Anitha, P. Kamalakkannan ,"Enhanced Cluster Based Routing Protocol for MobileNodes in Wireless Sensor Network" In Proceedings of 2013 International Conference onPattern Recognition, Informatics and Mobile Engineering (PRIME), 2006, pp. 187-193.

[27] Samera. B. Awwad, cheekyunng and Nor K. Noordin "Cluster Based Routing (CBR) Protocol with Adaptive Scheduling for Mobility and Energy Awareness in Wireless Sensor Network," In Proceedings of Proceedings of the Asia Pacific Advanced Network,2009, pp 34-46.