ISSN: 2278 – 7798
International Journal of Science, Engineering and Technology Research (IJSETR)
Volume 5, Issue 4, April 2016

Review on Cryptographic Schemes for Wireless Sensor Network

Neha Hans[1], Ms. Neha Goyal[2],

M-Tech Student[1], Assit. Prof.[2] & Department of CSE & Shri Ram College of Engg. & Mgmt
Palwal, Haryana, India

ABSTRACT
Wireless Sensor networks (WSN) contains hundreds or thousands of low power, low cost and self-configuring nodes which are highly distributed. Because of the cause that the sensor nodes are highly distributed, there is a requirement of network security. Security is a significant problem nowadays in almost each network. There are several security problems and various attacks that required to be seeing around and work upon. QoS and Security is the major concern in WSN because of its wireless communication constraints and nature i.e. less memory, low computation capability, vulnerability to physical capture or damages, bounded energy resources and the usage of insecure wireless communication channels. These restraints build security along with the QoS, an issue in WSN. The cryptographic techniques increase the level of security and build it protected against serious attacks but also have a important effect on the QoS of WSN.

Keywords— Wireless sensor Networks, Security Concerns, QoS, ANODR, Cryptography, IPSec, WSN's, ISAKMP.

I. INTRODUCTION

Wireless sensor networks (WSNs) are consisted of large no. of densely deployed sensors. A key characteristic of these networks is that their nodes are unavailable. WSNs can be used in a broad variety of applications needing either a particular kind of sensor or a mixture of sensor types [2]. The class of environmental monitoring applications concentrates on physical variables i.e. lighting conditions, temperature, motion, noise, object presence and mechanical stress. The class of surveillance applications concentrates on determining location sensing, crucial events and object tracking. Hence, for example, homogeneous WSNs could be used to monitor vibrations and focuses on a large structure i.e. oil rig or a ship. On the other side, homeland security applications would need a heterogeneous WSNs containing of various types of sensors involving biochemical sensors, radiation sensors and digital video cameras, managed by a set of base stations [3]. Other potential target domains for heterogeneous WSNs involve habitat monitoring, battlefield surveillance and health monitoring.

Types of Sensor Networks

A. *Terrestrial WSNs*

In these, nodes are distributed in a provided region either in an ad hoc way (sensor nodes are randomly positioned into the target area by discarding it from plane) or in pre-planned way (sensor nodes are positioned according to optimal placement, grid placement, 2-d and 3-d placement models). However battery power is restricted and it cannot be recharged, terrestrial sensor nodes must be offered with an optional power source i.e. solar cells [4].

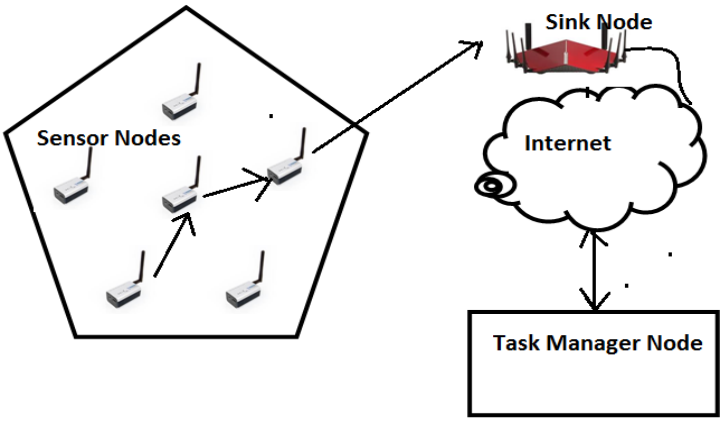

Figure 1: Wireless Sensor networks (WSN)

B. *Underground WSNs*

In these, sensor nodes are forgotten underground or in a mine or cave that monitors the underground situations. Sink nodes are positioned above the ground to send the collected information from the sensor nodes to the base station. These are more costly as compared to the terrestrial sensor networks because suitable nodes are to be chosen that can confirm reliable communication through rock, soil, water and other mineral contents [3].

C. *Underwater WSNs*

In these, vehicles and sensor nodes are positioned underwater. Autonomous vehicles are utilized for collecting the data from the sensor nodes. Sparse deployment of nodes is performed in this network. Main issues that come under this while communicating are long propagation delay, restricted bandwidth and signal fading issue [4].

D. *Multimedia WSNs*

In these, low cost sensor nodes are fitted with microphones and cameras. These nodes are positioned in a pre-planned way to confirm coverage. Problems in these networks are requirement of high energy consumption, high bandwidth, data processing, quality of service provisioning and compression mechanisms, and cross layer design [7].

II. Literature Review

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.

III. CRYPTOGRAPHIC SCHEMES FOR WIRELESS SENSOR NETWORK

Wireless sensor network are susceptible to various kinds of attack that influence the performance such as QoS of wireless sensor network. To neglect this, various kinds of security mechanisms depending on cryptography are employed to wireless sensor network to prevent it from these attacks. These techniques have important effect on the network QoS.

A. Internet Protocol Security (IPSec)

IPSec is a collection of protocols proposed by Internet Engineering Task Force (IETF) to offer security for a packet at network level. IPSec supports to generate authorized and trusted packets for IP layer.

Modes of IPSec Protocol

IPSec works in one of two different modes such as transport Mode and tunnel mode.

a. Transport Mode: In this mode, IPSec secures the data content that is provided from the transport layer to the network layer. The transport mode secures the network layer payload by encapsulating it. Transport mode does not secure the IP header. In other words the transport mode does not secure the complete IP packet; it secures only the packet from the transport layer. The IPSec header and trailer are both joined to information that is coming from transport layer after that IP header is joined. The transport mode is usually utilized when we require host to host security of data. The sender utilizes IPSec to authorize and/or encrypt the pay load provided from transport layer. The recipient utilizes IPSec to examine the authorization and /or decrypt the IP packet and provide it to the transport layer [5].

b. Tunnel mode: In this mode, IPSec secures complete IP packet. It takes an IP packet, involving the header, employs IPSec security mechanism to the whole packet, and then joins a new IP header [7]. This new IP header has different information than the real IP header. The tunnel mode is utilized between a router and a host, between two routers, or between a host and a router. In other words, we utilize the tunnel mode when either the receiver or the sender is not a host. The whole original packet is secured from intrusion between receiver and sender. It is as if the entire packet goes through an imaginary tunnel.

Security Protocols in IPSec

IPSec frameworks consists two protocols such as and the Encapsulating Security Payload (ESP) Protocol and the Authentication Header (AH) protocol to offer encryption and/or authentication for packet at the IP level.

a. Encapsulating Security Payload (ESP): It offers integrity, authentication and confidentiality, which secure the data from tampering and most effectively, offer message content security. IPSec offers an open framework for implementing industry standard algorithms i.e. MD5 and SHA. The algorithms, that IPSec utilize to create a unique and unforgivable identifier for each packet, which is a data equal to a fingerprint. This fingerprint permits the device to confirm whether the data packets have been modified or not. Moreover, packets that are not trusted are dropped and not provided to the authorized recipient. It also offers all encryption facilities in IPSec [8]. The encryption technique interprets the readable message (data) into an unreadable format that completely encapsulates the message content that cannot be understood by any intruder. The decryption, interprets the message content from an unreadable format to a readable message. Encryption/decryption permits only the authenticated receiver/sender to read the data. In summation to this, the ESP has another alternative to perform authentication, known as ESP authentication. This ESP authentication offers integrity and authentication for the payload and not for the IP header. In the current work, in ESP, the DES-CBC algorithm is utilized for encryption/decryption and HMAC-MD5 for the authentication. DES is a cipher block. It translates data in block, each of size 64 bits. In this the plain text of size 64 bits goes as the input to DES, which generates 64 bits of cipher text. The key length is 56 bits [9].

b. Authentication Header (AH): The authentication header protocol is intended to authenticate the source host and to confirm the payload integrity carried in the IP packet. The protocol utilizes a symmetric key and a hash function to produce a message digest; the digest is introduced in the authentication header. The AH is then positioned in suitable location depending on the mode. When an IP datagram takes an authentication header, the original value in the protocol field of IP header is substituted by another value. The field inside the authentication header (the next header field) keeps the actual value of protocol field (the type of payload being carried by the IP datagram).

IV. 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.

IV. Energy Efficient Session Key Establishment (EESK) Network Model

There are three types of wireless devices are available in our model: cluster head nodes (CH), sink node/base station (BS) and wireless sensor nodes (S).

Sensor nodes (S): Sensor nodes are resource constraints; every sensor only has restricted memory storage, power and short radio transmission range. Sensor nodes only interact with their cluster head directly; no interaction between sensor nodes available. Sensor nodes are stationary after the deployment.

Cluster head nodes (CH): in comparison with sensor nodes, cluster heads have substantially high energy resources. They are fitted with large memory storages, high power CPUs and radio transmission range. Cluster heads can interact with each other directly, and relay information among sink nodes and sensor nodes.

Sink node/Base station (BS): Sink node is the most strongly node in a network. It has virtually unrestricted communication and computational power, unrestricted memory storage, and very large radio transmission range to arrive all the sensors in the network.

In our network model, a huge no. of sensors are randomly distributed in a region. Sink node is deployed in a well-secured place. As illustrated in Figure 2, CHs divides the sensors into different clusters by many clustering algorithm, for example every cluster has a set of sensors and a cluster head; cluster head collects the data from sensors, performs mission-related data processing, and forwards the processed data to the sink node [12].

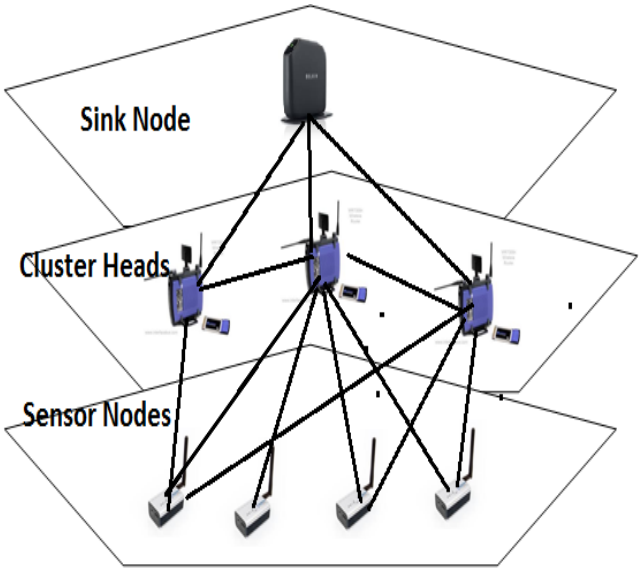

Fig.2. A hierarchical wireless sensor network architecture

V. STANDARDS OF WSNS SIMULATORS

There is a no. of authentic bodies which adjust performance standards in an area of WSNs bodies. These bodies manage their mentioned standards time to time to maintain the pace with current needed frame. Many standards are currently either signed or under development. The IEEE concentrates on the MAC and physical layers; the Internet Engineering Task Force operates on layers three and above. In summation to these, bodies i.e. the International Society of Automation offer vertical solutions, covering all protocol layers. At last, there are also many non-standard, proprietary techniques and specifications. Standards are utilized far less in WSNs as compared to other computing system which builds most systems incapable of direct interaction among different systems. Since predominant standards often utilized in WSN communications involve [11]:

- Wireless HART
- IEEE 1451
- Zig Bee / 802.15.4

A. Wireless HART

Wireless HART is a wireless sensor networking technique depending on the Highway Addressable Remote Transducer Protocol (HART). All nodes are a Wireless HART network is full-function devices able of routing multi-hop traffic [11, 12]. Hence all Wireless HART networks make full mesh network configurations. The protocol uses a self-organizing and time synchronized architecture. The protocol provides support to operation in the 2.4 GHz ISM band utilizing IEEE 802.15.4 standard radios. Formulated as a interoperable, multi-vendor wireless standard, Wireless HART was described for the needs of process field device networks.

The standard was started in early 2004 and formulated by 37 HART Communications Foundation (HCF) companies that amongst others involved Emerson, ABB, Pepperl+Fuchs, Endress+Hauser, Siemens which build WiTECK a non-profit, open membership organization whose objective is to offer a cost-efficient, reliable, high-quality portfolio of core enabling system software for industrial wireless sensing applications, under a company and platform neutral umbrella. The fundamental wireless technique depends on the work of Dust Networks; TSMP (Time Synchronized Mesh Protocol) technique. It also considers that wireless assets will be deployed where wired assets are hard to place, so that Wireless HART devices must be capable to run for a long time on a single set of batteries. The basis of the Wireless HART MAC is time division multiple access (TDMA) to the channel, instead of the CSMA-CA mechanism considered by the 802.15.4 MAC. In fact, data transport in a well-built Wireless HART network is generally more than 3-sigma (99.7300204%) reliable, and under normal situations is more than 6-sigma (99.9999998%) reliable.

B. IEEE 1451

IEEE 1451 is a set of smart transducer interface standards formulated by the Institute of Electrical and Electronics Engineers (IEEE) Instrumentation and Measurement Society's Sensor Technology Technical Committee that explain a set of common, open, network-independent communication interfaces for linking transducers (actuators or sensors) to instrumentation systems, microprocessors and control/field networks. One of the key factors of these standards is the definition of transducer electronic data sheets (TEDS) for every transducer. The TEDS is a memory device linked to the transducer, which saves transducer calibration, identification, correction data and manufacturer-related information. The objective of the IEEE 1451 family of standards is to permit the access of transducer data by a common set of interfaces whether the transducers are linked to systems or networks through a wireless or wired means. The 1451 family of IEEE Standard for a Smart Transducer Interface for Sensors and Actuators with their features is provided in Table 3.

TABLE III IEEE 1451 STANDARD ALONG WITH THEIR PROPERTIES

IEEE Standards	Properties
1451.0-2007	Common functions, Communication Protocols, and Transducer Electronic data sheet (TEDS) Formats
1451.1-1999	Network Capable Application Processor Information Model
1451.2-1997	Transducer to Microprocessor Communication Protocols & Transducer Electronic Data Sheet (TEDS) Formats

1451.3-2003	Digital Communication & Transducer Electronic Data Sheet (TEDS) Formats for Distributed Multi-drop Systems
1451.4-2004	Mixed-Mode Communication Protocols & TEDS Formats
1451.5-2007	Wireless Communication Protocols & Transducer Electronic Data Sheet (TEDS) Formats
1451.7-2010	Transducers to Radio Frequency Identification (RFID) Systems Communication Protocols and Transducer Electronic Data Sheet (TEDS) Formats

C. ZIGBEE / 802.15.4

ZigBee is a specification for a suite of high level communication protocols utilizing low-power, small digital radios depending on an IEEE 802 standard for personal area networks (PAN). Zig Bee devices are usually utilized in mesh network form to transmit data throughout longer distances, passing data through intermediary devices to arrive more distant ones. This permits Zig Bee networks to be built ad-hoc, with no centralized control or high-power transmitter/recipient capable to arrive all of the devices. Any Zig Bee device can be assigned a task with running the network. Zig Bee is aimed at applications that need a long battery life, low data rate and protected networking. Zig Bee describes three classes of devices: Zig Bee Routers (ZR), ZigBee Coordinators (ZC) and Zig Bee End Devices (ZED). Every network has one ZC, which is responsible for formation of network [11] and which can also help in message routing. ZR's also play role in routing and can operate a sensing/ actuation application as well. ZED's only operate applications and cannot play role in message routing — every ZED must inform to either a ZC or the ZR. Applications involve electrical meters with in-home-displays, wireless light switches, traffic management systems and other consumer and industrial resources that need a short-range wireless transfer of data at comparatively low rates. The technique described by the ZigBee specification is designed to be simpler and less costly as compared to other WPANs i.e. Bluetooth [12].

CONCLUSION

In this paper, we introduce a brief review on wireless sensor network, its features and its types. Then we talked about the sensor networks security, security problems and several DoS attacks on various layers. Security is a significant need and complicates enough to adjust in different domains of WSN. We also talk about several dimensions of security (integrity, availability, authenticity and confidentiality) that are being directed by several physical attacks.

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.

[28] R. Balasubramaniyan , Dr. M. Chandrasekaran "A New Fuzzy Based Clustering algorithm for Wireless Mobile Ad-Hoc Sensor Networks "In Proceedings of 2013 International Conference on Computer Communication and Informatics,2013, pp 31-37