American Journal of Sensor Technology, 2014, Vol. 2, No. 3, 34-39
Available online at http://pubs.sciepub.com/ajst/2/3/2
© Science and Education Publishing
DOI:10.12691/ajst-2-3-2

Energy Efficient Secure Firewall and Packet Filtering System in Wireless Sensor Networks

Manjuprasad B[1,*], Andhe Dharani[2], Shantharam Nayak[3]

[1]Research Scholar, Department of ISE, R.V. College of Engineering, Bangalore, INDIA
[2]Associate Professor, Department of MCA, R.V. College of Engineering, Bangalore, INDIA
[3]Professor, Department of ISE, R.V. College of Engineering, Bangalore, INDIA
*Corresponding author: manjuprasad32@gmail.com

Received June 03, 2014; Revised June 13, 2014; Accepted June 18, 2014

Abstract Sensor networks play a key role in collecting information from the human unattended and surveillance area. The information collected from any types of networks should be secure in all perspective and that too security in sensor networks is crucial because the information is of auto generated type and it is difficult to distinguish between original and replicated information at receiver side. The existing secure mechanism like cryptographic techniques is too complex and it affects the performance of the sensor networks by dissipating more energy for both computational and communicational purpose. This research work aims to propose a low complex simple secure mechanism for sensor networks which can withstand the simple types of attacks to provide a framework for achieving Confidential, Authentication and Integrity. This security is achieved by adopting a firewall rules and packet filtering in the sensor networks with an efficient clustering mechanism for the resource constrained sensor devices.

Keywords: *wireless sensor network, LEACH, clustering, key compression, data authentication, confidentiality, integrity*

Cite This Article: Manjuprasad B, Andhe Dharani, and Shantharam Nayak, "Energy Efficient Secure Firewall and Packet Filtering System in Wireless Sensor Networks." *American Journal of Sensor Technology*, vol. 2, no. 3 (2014): 34-39. doi: 10.12691/ajst-2-3-2.

1. Introduction

Wireless Sensor Networks (WSNs) are a hodgepodge of numerous tiny low cost and limited resources nodes which are connected through some wireless link like 802.15.1, 802.15.4 and other wireless standards. These tiny nodes are the collection of many components such as sensors for sensing, battery for power supply, memory for data storage, processor for performing different operations, transducer for radio communication purposes. These nodes will forward the collected data to the centralized base station with some intermediate nodes.

These devices are mainly deployed for monitoring and tracking application in the human untended areas like forest and battle field [1] where human monitoring is not feasible. The major snag in WSNs is the limited resources like battery, memory and processing power. There is a feasible option for power optimization by harvesting the energy from the environment like solar energy but security issues cannot be neglected.

Currently there are many protocols for efficient resource utilization which operates on different OSI layers but data link and network layers drawn more attention in WSNs. MAC protocols is one of the efficient methods which concentrate on the Data link layer by imposing low duty cycle [2,3] and TDMA [4]. Apart from this routing plays a vital role in efficient data transmission, one of the optimal solution used for routing in WSNs is clustering. [5] [6]. The clustering mechanisms [7,8] can be implemented for varying network topology [9,10] by imposing topology control and other [11] energy saving mechanisms which increases the lifetime of the WSNs.

The need of security in WSNs is plays a vital role due to the nature of communication. The data transmission in WSNs is done by using standard wireless technology like Zigbee, Bluetooth, 802.11 etc. Due to the broadcast nature of the WSNs the data transmitted can be easily received by any types nodes where some of the nodes may be malicious. So there is necessary of providing security in WSNs for providing various security requirements like confidentiality [12], quality and availability [13] of the original information [14].

Confidentiality: The data that is processed by the sensor nodes which is to be sent to other trusted nodes must be kept in secret from any unauthorized entities in the network. The standard approach for confidentiality is to encrypt the data with a secret key that should be able to use only by the authorized personal. But cryptography is too expensive to apply for the resource constrained sensor nodes.

Integrity: Integrity means that the message that is being communicated by the trusted nodes should be un-altered during the transmission from a source to destination node by any malicious node. This is usually done in conventional network using MAC (Message Authentication Code) or digital signatures.

Authentication: Is the process of identification that the receiving nodes are sure that the message it receives comes from a legal source and the sending nodes ensure that the message is received only by the authorized nodes.

WSNs are more vulnerable to the attacks made by the malicious nodes, so providing security in wireless sensor networks is a complex task because of the various types of attack that make a security requirements complex. The Attacks on wireless network can be broadly divided into 3 main classes as shown below [15,16]:

Interception is an attack on confidentiality where the sensor nodes are compromised by an opponent node to gain unauthorized access to malicious node example for this type of attack is Eavesdropping. This attack can be said as passive attacks because there will be no loss and the attacker can only read the information without injecting any false packets.

Modification is an attack on integrity. Modification means an unauthorized node not only read the data but tampers the data with some false packets; example for this attack is packet sniffing which is considered as active attack.

Fabrication is an attack on authentication. An adversary node injects false data and tries to compromises to share the information transmitted. This causes the nodes to changes its original behavior, example for this attack is injecting false message.

All types of attack s in WSNs will comes under the above 3 main category. The brief description of the various types of attacks [17,18] is discussed below.

Hello Flood Attack: A malicious node will send a strong signal of Hello message to the nodes in the network so the nodes will think that this node is very near to it and send its data to this node but actually the node is not in the network so there will be a loss of that data and energy

Replay Attack: A malicious node stores a received message and attempts to send it at later time, when nodes receive the message they believe that is original message and cause that node to come with a wrong distance.

Sybil Attack: The malicious node will appears to be in the set of a node and send wrong information to other nodes.

Sinkhole Attack: The malicious nodes attract all the traffic from certain area and appear to be as base station so that all members will go towards this instead of sink.

The major Security Challenges [18,19] in WSNs are:

Minimizing resource consumption and maximizing security performance.

Sensor network deployment renders more link attacks ranging from passive eavesdropping to active interfering.

In-network processing involves intermediate nodes in end-to end information transfer.

Large scale and node mobility make the affair more complex.

The rest of the paper is structured as follows. Section II presents the current related work in the field of WSNs for efficient power optimization and security solutions. Section III presents the proposed mechanism for achieving a simple security in WSNs. Section IV focused on the results and simulation details. Section V concludes the objective of this work.

2. Related Work

This section presents the analysis done on the different existing efficient security and power optimization mechanisms in wireless sensor network.

2.1. Power Optimization

Power optimizing is one of the major sang in WSNs as there is no feasible option for replacing or recharging the battery of the nodes. One of the main reasons for battery failure is, its size but it is necessary to reduce the size of the battery for making the tiny sensor nodes which are very useful in surveillance type applications. The brief discussions on some of the existing power optimization mechanism which are more cited and published is superior journal are discussed below.

2.1.1. A Low Energy Time Based Clustering Technique for Routing in Wireless Sensor Networks [20]

A distributed clustering based routing protocol for WSNs is proposed based on the residual energy based clustering [21] technique where the selection of cluster head is decided by its residual energy. The probability of the number of nodes becoming cluster head is decided by the number of alive nodes in the network. This mechanism is implemented for heterogeneous WSNs where some probability of the nodes is assumed to be having more energy than others. This time based clustering has got better lifetime enhancement.

2.1.2. Low-Energy Adaptive Clustering Hierarchy (LEACH)

It is a self-organizing and adaptive clustering protocol proposed in [6]. The operation of LEACH is divided into rounds, where each round begins with a setup phase for cluster formation, followed by a steady-state phase, when data transfers to the sink node occur. It uses random election of cluster heads to achieve load balancing among the sensor nodes. In LEACH a sensor node is elected as the cluster head according to a distributed probabilistic approach. Non cluster nodes decide which cluster to join based on the signal strength. Based on the distance of the cluster head the non sensor node select or join the cluster head which is nearest to them.

2.1.3. ELMO: Energy Aware Local Monitoring in Sensor Networks [22]

This protocol provides a high-performance energy-efficient monitoring for wireless sensor networks. By using three different mechanisms for optimizing the power consumed in WSNs with synchronized sleep-wake, continuously acting and triggered WSNs. This sleep wake methods is done in a secure manner with low energy dissipation.

One of the major factors that affect the performance in terms of power is topology of the network. The architecture [23] of the network topology should be designed for all feasible scenarios. This is achieved by designing tier architecture in WSNs.

2.2. Security Mechanism

Security is another important issue in all the fields, wireless sensor networks is not an exception to this.

Security in sensor networks can be achieved by maintaining data confidentiality, authentication, freshness and integrity. One of the main mechanisms used for this purpose is encryption and decryption but due to resource constraints in sensor nodes these mechanism will affect their performance and increases the computational complexity of the nodes.

2.2.1. Agent-based Trust Model in Wireless Sensor Networks [24]

This focused on providing a security in WSNs using an agent based trust model. This agent nodes will independently monitors the behavior of the nodes within its range and broadcast their trust rating to the authenticated nodes. By this broadcast it is possible to minimize the effect of the malicious node like bad mouthing attack, on off attack and conflicting behavior attack. This agent based method provides a more accurate result along with cryptographic mechanisms to detect the malicious node in WSNs.

2.2.2. Simple Secure Protocol

This protocol [25] provides a simple security solution for an efficient information transmission in WSNs with low computational complexity and efficient resource utilization in wireless sensor networks. This is achieved by deploying dedicated nodes for monitoring the networks and alerting the original nodes about the presence of malicious nodes by this way the information collected is authenticated. Once this is achieved each cluster head will compress the data with a key know only to base station for providing a confidentiality. This mechanism is achieved in energy efficient way too. Table 1 shows the energy dissipation during various operations.

Table 1. Energy Dissipation of SSP

Operations	Proposed SSP Approx Energy (mJ)
CH to DNS	0.56
DNS to CH	2
DNS to Members Node	*6*
Key Compression at CH	5
Total energy cost	13.56

2.2.3. An ECC-Time Stamp based Mutual Authentication and Key Management Scheme for WSNs [26]

This work proposed an energy and memory efficient key management by using a unique session key for different phases with a generation of the session password. This mechanism uses an Elliptic Curve Arithmetic with highest cryptographic strength for each bit among many existing public key cryptosystems. This scheme is implemented with lower power and memory requirements by saving the bandwidth.

3. Proposed Work

The main motivation for this proposed work is the computational complexity and resource constraints that are affecting the performance of WSNs. In many of the research work there is no clear illustration on both efficient security and clustering process some are focused only security and some are on energy optimization. The proposed work aims to focus on both the parameters by proposing a heterogeneous secure clustering mechanism. This work is the enhancement of our previous work discussed in section II [25]. The working of the proposed mechanism is discussed below.

3.1. Efficient Cluster Formation

Clustering is one of the efficient mechanisms in sensor networks. This work proposes a new clustering mechanism for balancing the energy over the network and increase the lifetime of the sensors by making heterogeneous based clustering. The probability of nodes becoming cluster head are not predefined unlike some of the existing cluster mechanisms like LEACH [6], UMCLCO [27], instead it is defined by the number of nodes associated in its surrounding area.

The network is deployed with some probability of nodes having more energy than others and these advance nodes will act a cluster head for more number of rounds. The criteria for selecting the cluster head is discussed below.

3.1.1. Threshold Distance for Selecting Cluster Head

To avoid the communication overhead at the Cluster Head (CH) a new threshold region is proposed as shown in the below equation for a hexagonal cell structure where R is a radius of hexagonal and r is a threshold distance within which no cluster head will be formed.

$$\mathbf{r} = \left(\mathbf{1}/\mathbf{4}\right)\mathbf{R}\sqrt{3} \qquad (1)$$

This method of selecting CH will distribute the cluster head uniformly over the network by reducing the communication overhead at the cluster head and base station (BS) by efficient use of TDMA.

3.1.2. Threshold Energy for Selecting Cluster Head

The node which is decided to become a cluster head must have some minimum amount of energy so that it can transmit the packet successfully to the base station. In a typical condition there is a chance of unsuccessful data transmission because a node might have some minimum energy that is sufficient to receive the data from receiver but may fail to transmit it to base station. This typical condition may also misuse the minimum amounts of energy present in the node instead it could be served as a member and utilize the energy efficiently as a member. This algorithm aims to calculate a threshold distance and the threshold energy for the node to become CH so that only the node satisfying this threshold energy will become a cluster head. Equation below gives the threshold distance and energy [23]:

$$M\varepsilon = \left(\varepsilon tx * \varepsilon da\right) * k + \varepsilon\, fs * k\left(Td * Td\right) \qquad (2)$$

Where,

$$Td = \sqrt{Md^2 + Md^2} = \text{Threshold distance}$$

$$Md = \frac{a}{400}$$

a= area of a Square network
εtx= Transmitting energy
εda= Data Aggregation Energy

k= Packet size

Electing a Eligible Nodes as Cluster Head

```
Step1: Find the Residual Energy of all the nodes
Step2: for I=1to N nodes
IF the nodes are Selected Nodes
IF Residual Energy (node I) >
Node (I) is elected as Cluster Head
ELSE
Node (I) is not a selected as a Cluster Head
End
Else
Goto Step2
End
```

Figure 1 shows the initial network model where the heterogeneous nodes are represented as circle and normal nodes as ‘x’.

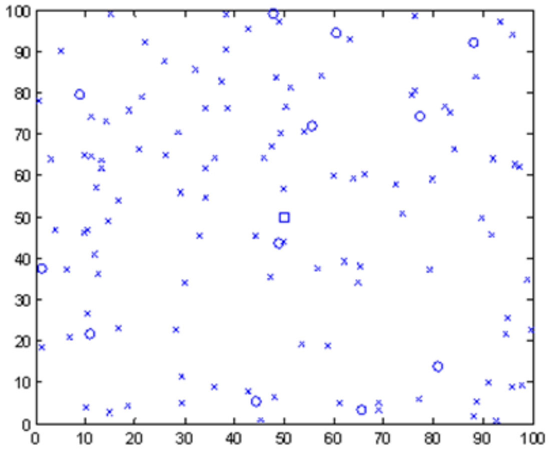

Figure 1. Initial Network Model

3.2. Secure Information Transmission

This phase concentrate on achieving the security requirements to withstand the some of the attacks in WSNs like eavesdropping, hello flood, DOS, Packet Sniffing.

Security level Assumptions considered:

In the Initial of the deployment there will be no malicious nodes considered in the network.

For testing purpose some malicious nodes are deployed in the network after some interval of time as shown in Figure 2 in red circle.

These malicious nodes are functioned only to send the false information, packet sniffing and to make hello attack.

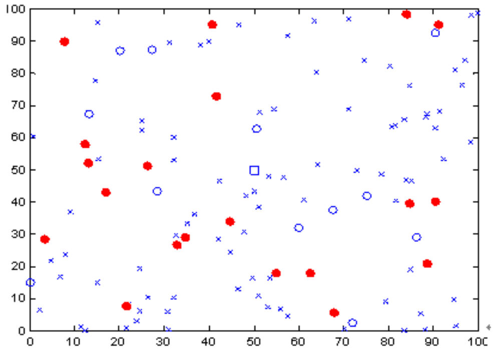

Figure 2. Network Model after deploying malicious nodes

Using these types of attacks the proposed mechanisms concentrates to provide data authentication, data confidentiality and data integrity for efficient information transmission. The brief working of this mechanism in discussed below.

The nodes will send a request to join a cluster nearest to it with its id. Information of all the nodes is known to the entire Cluster heads in the network through base station. The cluster heads will verify the nodes based on the pre-registered id. After the verification the cluster head sends an acknowledgement to the members with some random id and stores both node id and the random id of each member for future security monitoring purpose.

3.2.1. Data Authentication

Using the initial information the cluster head will achieve the data authentication using the following basic firewall rules.

Rule-1: The nodes ID's or IP’s must be pre-registered

Rule-2: The node random ID's acknowledge from cluster head should match with node ID's.

Rule-3: The information from the nodes with Invalid ID's or IP's and random ID’s are filtered by each Cluster Heads.

Figure 3 shows the data transmission during the cluster phases where the malicious nodes are filtered by the proposed set of firewall rules. The unauthorized transmissions by the malicious nodes are blocked at the cluster head which is indicated in red color. This filtering will processed at the cluster head side where the cluster head is assumed to be having more energy due to heterogeneous deployment scenario.

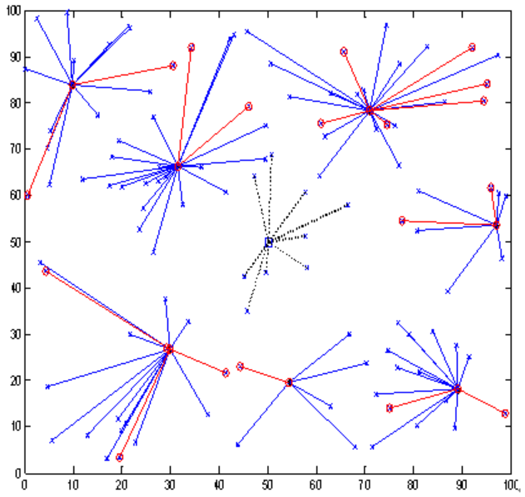

Figure 3. During Transmission Phase

3.2.2. Data Confidentiality

Once the cluster head receives the information from its members it will compress the data into single packet encrypted with a key known only to the base station. This way of packet transmission will prevent eavesdropping of the information from the malicious nodes.

3.2.3. Data Integrity

This security requirement plays a vital role in providing security as the data confidentiality and authentication may not sufficient in some types of attack like packet sniffing. In this attack the malicious nodes may inject false packet to the packet sent by original nodes and it is difficult to identify this because the packets may of authenticated ID's or IP’s with the injected false messages.

Packet Checking Bit: In order to verify the originality of the packets sent by the nodes there will be one extra bit indicating the originality of the message. The bit is set to 0 initially when the nodes sends the packet and 1 on addition of packets which is considered as duplicate packets injected by the malicious nodes. This method also restricts the original nodes to manipulate the messages. At every cluster head this bit will be checked before receiving the information from any nodes.

Confidential Integrity Authenticated Algorithm for WSNs (CIAWSN):-

Step-1: Heterogeneous based Cluster Head Selection

Step-2: Registration of Cluster members with ID's or IP's and random ID's.

Step-3: Verify the node ID's or IP's with random numbers for node Authentication

Step-4: Verify the Packet to identify the false packet injection for Data Integrity

Step-5: Encrypt the packets at Cluster head with key know only to Base station for information confidentiality.

The proposed algorithm focused on achieving the three major security requirements in WSNs. This work focused on providing low complex secure mechanism for resource constrained devices. The attacks can be neutralized by proposed mechanism as discussed below.

3.2.4. Resistance to Attacks

Eavesdropping: The entire message sent by CH's are encrypted using a secret key know to base station can prevent malicious nodes from reading the information.

Packet Sniffing: The usage of extra parity bit makes the nodes to identify whether the packets is altered or not.

False Message: The network will not get any false message due to the pre-registered nodes and node filtering technique.

4. Results and Discussions

The proposed secure protocol aims to provide a low complex security mechanism in WSNs to reduce the computational complexity and resource usage at the node side. The proposed algorithm is based on the clustering and it is achieved a better results than the LEACH with an added security features. Figure 4 shows the lifetime of the proposed and LEACH which is simulated and compared for the collected parameters as shown in Table 2 and it is 4% energy efficient than LEACH with secure data transfer.

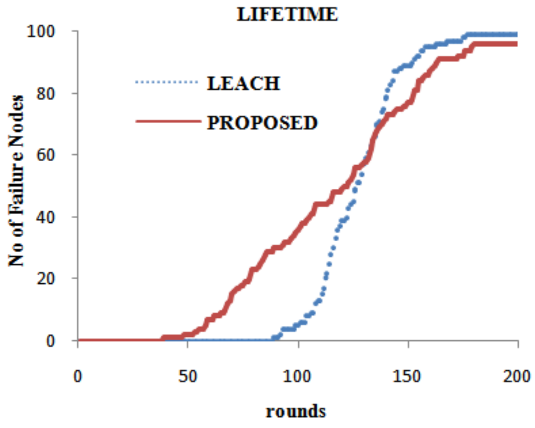

Figure 4. Network Lifetime

The proposed secure CIAWSNs mechanism achieved better results in providing a various security requirements like Confidentiality, Integrity, and Authentication. Figure 5 and Figure 6 shows the number of packet dropped from the identified malicious nodes deployed for testing purpose at base station and cluster head respectively.

Table 2. Energy Dissipation of SSP

Parameter	Value
Network grid	From (0,0) to (100,100)
Number of nodes	10
Sink	At (50,50)
Initial Energy of each node	0.05J
Data packet size	4000 bits
Data Aggregation Energy	5nJ/bit
Energy to Receive	50 nJ/bit
Energy to transmit	50 nJ/bit
Energy for checking Parity Bit	5nJ/bit
No of Malicious Node	20
Probability of Attack from Malicious Nodes	0.2
Simulated for	100 rounds

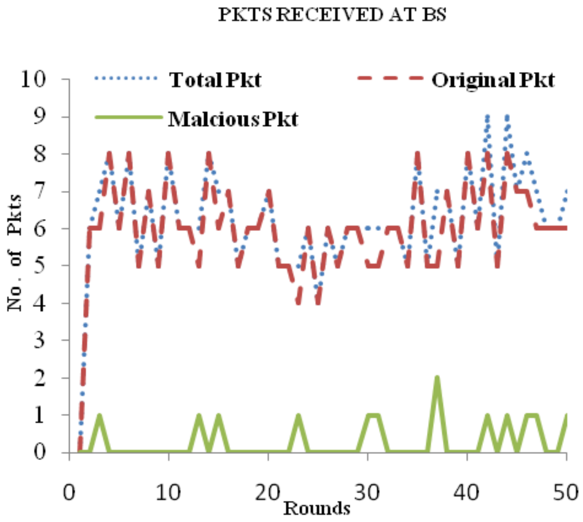

Figure 5. Packet Received at Base Station

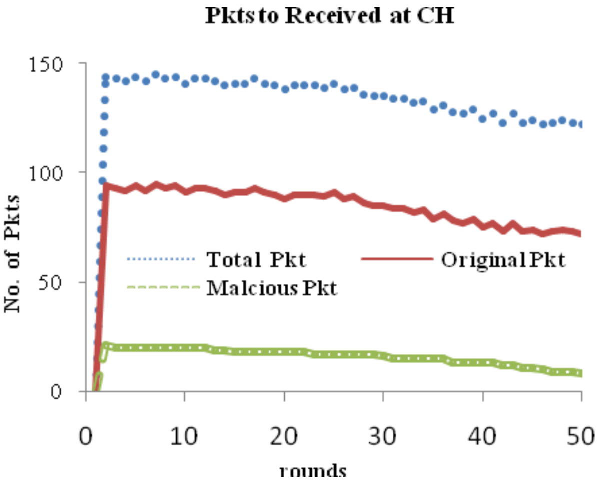

Figure 6. Packet Received at Cluster Heads

The main aim of this proposed method is to provide low complex secure and efficient power utilization. The above results show the achievements of the proposed work. Figure 7 shows the energy consumption of the proposed methods for with and without firewall rules. The result shows the energy consumption is negotiable with usage of firewall rules.

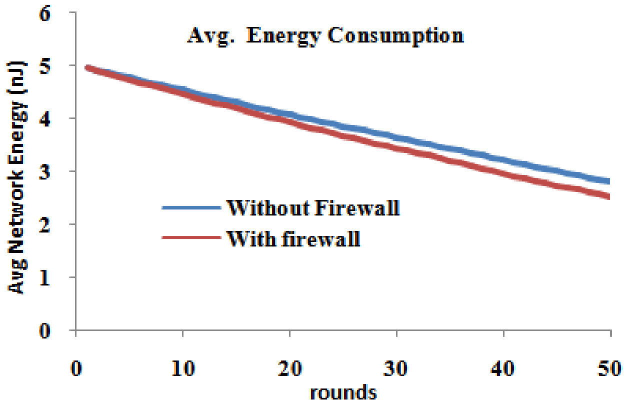

Figure 7. Avg Energy Consumption: with and without firewall

5. Conclusion

The proposed CIAWSNs focused on providing a simple low complex secure mechanism for resource constrained WSNs. This mechanism is able to achieve the major security requirements required in WSNs like confidentiality, authentication and integrity with low complex solutions. CIAWSNs also concentrated on power optimization which is a major snag in sensor networks. The proposed firewall rules are verified at the cluster head which is having more energy with packet filtering. This mechanism is having low complexity and can be operated at low operating cost for the resource constrained sensor nodes.

References

[1] Wendi B, Heinzelman, Anantha P, Chandrakasan, Hari Balakrishnan. *"An Application-Specific Protocol Architecture for Wireless Microsensor Networks"*. IEEE transactions on Wireless Communications, pp. 660-670, Oct.

[2] Sumit Kumar, Siddhartha Chauhan, *"A Survey on Scheduling Algorithms for Wireless Sensor Network"*, International Journal of Computer Applications (0975-8887) Volume 20-No. 5, April 2011.

[3] K.-J. Wong and D. Arvind. Speckmac: *"Low-power decentralized mac protocol low data rate transmissions in specknets"*. In Proc. 2nd IEEE Int. Workshop on Multi-hop Ad Hoc Networks: from Theory to Reality (REALMAN'06), May, 2006.

[4] D.M. Blough, M. Leoncini, G. Resta, and P. Santi." *The k-neighbors approach to interference bounded and symmetric topology control in ad hoc networks"*. IEEE Transactions on Mobile Computing, 5 (9): 1267 {1282, 2006.

[5] Manju Prasad, Andhe Dharani, "A QoI Based Energy Efficient Clustering for Dense Wireless Sensor Networks", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), ISSN 2231-4482, Vol 3, No. 2, April 2013.

[6] W. R. Heinzelman, A. Chandrakasan, and H. Balakrishnan. *"Energy efficient communication protocol for wireless microsensor networks"*. Hawaii International Conference on System Sciences, January 2000.

[7] Mohanaradhya, Sumithra Devi, Andhe Dharani,*" Distance Based cluster head selection in Wireless Sensor Networks*", International Journal Research in Emerging Technology, IAIEM, 2013.

[8] Meenakshi Diwakar1 and Sushil Kumar2, "*An Energy Efficient Level Based Clustering Routing Protocol For Wireless Sensor Networks*", International Journal Of Advanced Smart Sensor Network Systems (IJASSN), Vol 2, No. 2, April 2012.

[9] A.K. Daniel, Pooja Rathi, Aakansha Agarwal, and Amaresh Maurya, *"Energy Efficient Clustering Protocol for Sensor Networks Using Token Based Hotspot Technique"*, International Journal of Research and Reviews in Computer Science (IJRRCS), United Kingdom, Vol. 3, No. 2, ISSN: 2079-2557 April 2012.

[10] Min Chen ·Meikang Qiu Linxia Liao Jongan Park · Jianhua Ma, *"Distributed multi-hop cooperative communication in dense wireless sensor networks*", Springer Science Business Media, LLC 2010.

[11] Serdar Vural and Eylem Ekici, *"On Multihop Distances in Wireless Sensor Networks with Random Node Locations*", IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 9, NO. 4, APRIL 2010.

[12] G. Guimaraes, E. Souto, D. Sadok, J. Kelner,*" Evaluation of security mechanisms in wireless sensor networks"*, in: Systems Communications Proceedings 2005, pp. 428-433.

[13] Perrig, R. Szewczyk, V. Wen, D. Culler, and J. Tygar. *"Spins: Security protocol for sensor networks,"* In proceedings of Seventh Annual International Conference on Mobile Computing and Networks, July 2001.

[14] Anitha S Sastry, Shazia Sulthana, Dr. S Vagdevi, *Security Threats in Wireless Sensor Networks in Each Layer, Int. J. Advanced Networking and Applications, Vol: 04 Issue: 04 Pages: 1657-1661 (2013) ISSN: 0975-0290.*

[15] Manjuprasad B, Andhe Dharani, "*Necessitate for Security in Wireless Sensor Network and its Challenges*", International Journal of Research in Computer Applications & Information Technology, ISSN Online: 2347-5099, Volume 1, Issue 1, July-September, 2013, pp. 21-25.

[16] Anitha S Sastry, Shazia Sulthana, Dr. S Vagdevi, "*Security Threats in Wireless Sensor Networks in Each Layer*", Int. J. Advanced Networking and Applications, Volume: 04 Issue: 04 Pages: 1657-1661 (2013) ISSN: 0975-0290.

[17] Manju Prasad, Andhe Dharani, *"An Epigrammatic Study of some of the Fundamental Concepts in Wireless Sensor Networks*", International Journal of Emerging Technology and Advanced Engineering, Volume 2, Issue 9, September 2012, ISSN 2250-2459.

[18] Xiangqian Chen, Kia Makki, Kang Yen, and Niki Pissinou, *"Sensor Network Security: A Survey*". IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 11, NO. 2, SECOND QUARTER 2009.

[19] A. Perrig, J. Stankovic, and D. Wagner, *"Security in wireless sensor networks,*" Commun. ACM, Special Issue: Wireless sensor networks, vol. 47, pp. 53-57, 2004.

[20] Ouadoudi Zytoune, and Driss Aboutajdine, *"A Low Energy Time Based Clustering Technique for Routing in Wireless Sensor Networks." American Journal of Sensor Technology*, vol. 2, no. 1 (2014): 1-6.

[21] O. Zytoune, Y. fakhri and D. Aboutajdine, *"Time Based Clustering Technique for Routing in Wireless Sensor Networks"*. International Conference on Multimedia Computing and Systems (ICMCS), 7-9 April 2011. Pages: 1-4.

[22] Issa M. Khalil, *"ELMO: Energy Aware Local Monitoring in Sensor Networks"*, Ieee Transactions On Dependable And Secure Computing, Vol. 8, No. 4, July/August, pp 523-536, 2011.

[23] Andhe Dharani, Member, IAENG, Vijayalakshmi M. N, Sumithra Devi K. A, *"Power Optimization in Ad hoc Sensor Networks using Clustering Approach"*, Proceedings of the World Congress on Engineering 2011 Vol II WCE 2011, July 6-8, 2011, London, U.K.

[24] Haiguang Chen 1,2, Huafeng Wu2, Xi Zhou 2, Chuanshan Gao2,*" Agent-based Trust Model in Wireless Sensor Networks*", ACIS International Conference on Software Engineering, Artificial Intelligence, Networking, and Parallel/Distributed Computing, 0-7695-2909-7/07, pp 119-124, 2007 IEEE.

[25] Manjuprasad B, Andhe Dharani, *"Simple Secure Protocol for Wireless Sensor Networks", World Congress on Computing and Communication Technologies, WCCCT-2014*, Trichy, on 27th Feb-1st Mar, 2014, pp 260-263, ISBN: 978-1-4799-2876-7/14 $31.00 © 2014 IEEE.

[26] Gaurav Indra, Renu Taneja, *"An ECC-Time Stamp based Mutual Authentication and Key Management Scheme for WSNs*", 27th International Conference on Advanced Information Networking and Applications Workshops, 978-0-7695-4952-1/13 $26.00 © 2013 IEEE.

[27] Manjuprasad B, Andhe Dharani, *"Uniform Multihop Clustering for Low Communication Overhead"* in Sensor Networks, Emerging Trends in Communication, Control, Signal Processing & Computing Applications (C2SPCA), 2013 Bangalore on, 10-11 Oct-2013, pp 1-4, 978-1-4799-1082-©2013 IEEE.