ISSN (Print) : 0974-6846
Indian Journal of Science and Technology, *Vol 9(36), DOI: 10.17485/ijst/2016/v9i36/92866, September 2016* ISSN (Online) : 0974-5645

WDT-CH: Watch Dog Timer Cluster Head Node based Sensor Node - Master Operations in Wireless Mobile Ad-Hoc Networks (WMAN)

G. Venkata Swaroop[1*] and G. Murugaboopathi[2]

[1]Department of Computer Applications, St. Peter's University, Avadi, Chennai - 600054, Tamil Nadu, India; venkataswaroop.g@gmail.com
[2]Department of Computer Science and Engineering, Kalasalingam University, Srivilliputtur - 626126, Tamil Nadu, India; gmurugaboopathi@klu.ac.in

Abstract

Objectives: To increase the security level with improved energy efficiency for emerging application developed under Wireless Mobile Ad-Hoc Networks. **Method/Statistical Analysis:** In order to get the increased level of security and energy efficiency, a WDT-CH (Watch Dog Timer based Cluster Head) node is deployed to do master operation of the WMANET. This WDT-CH is increasing the network lifetime by handling network's master operations. The network is constructed by deploying the random nodes in cluster basis. As more number of clusters is created, a stipulated number of nodes can be placed in each cluster in equal manner. WDT-CH is a watch dog timer based CH node which acts as a station keeping node. In each level, there is a main selection and redundant selection of WDT-CHCH node. At a time, one node is taken to monitor the other nodes in each cluster. By this, all nodes have health status in different clusters by the help of maintaining the status word. Also Master operations are included for obtaining node information through status word. Routing tree is used to discover the path for data communication and encryption technique in the path is used from source to sink via Key Distribution Centre (KDC). All these operations are managed by WDT-CHCH node and sensor nodes. **Findings:** The entire proposed approach is simulated in Network simulator software and it reveals, how effectively energy level is maintained in the network. By implementing the WDT-CH algorithm, routing tree and secured key based encryption methods the overall throughput, Packet Delivery Ratio (PDR), End-to-End delay and energy may be effectively managed. **Application/Improvements:** The simulation was compared with the existing approaches and found that the Packet Delivery Ratios increased to 0.18% than the existing research works.

Keywords: Clustering, Energy Efficiency, Mobile Ad-Hoc Network, Watch-Dog-Timer Based Cluster Head

1. Introduction

Wireless Mobile Ad-Hoc Networks (WMANs) provide more supportive services having the best effort in real-time surveillance due to its prevalence. These networks need to provide Quality of Service in terms of bandwidth, less energy consumption and less delay. In[1], discussed about distributing the traffic to save the node energy where it avoids node early expiration due to overload. To do this, load balancing is combined with the energy aware routing mechanism called as Path Efficient and Energy Aware Ad Hoc Multipath Distance Vector (PE-EA-AOMDV) routing protocol. In[2], a novel video steganography method is applied by integrating Haar Integer Wavelet Transforms (IWT) and Least Significant Bits (LSB) substitution for hiding the data over RGB channels extracted from video file. This process is carried out on text binary form of the data. Power consumption is reduced by applying a novel power management system where it utilizes a pack of two solar powered batteries and automatic battery switching system. This battery system is used to replace the real time battery used in the node[3]. But this battery replacement system is used only in certain kinds of applications. In[4] reported that the link

* *Author for correspondence*

capability, power management and mobility management can be obtained by a suitable deployment of nodes within the network coverage area.

Wide range of applications are deployed and utilized under WMANs like surveillance monitoring[5–7] security[8,9] sensing in military, home automation, healthcare[10] and traffic monitoring etc. A usual WMAN contains huge number of sensor nodes with a sink node. A sensor node is small in size, having ability to sense and communicate with other sensor nodes in the same/different networks under same frequency remotely. Since the sensor nodes are deployed in remote environments energy becomes the critical issue in WMAN where the sensor nodes are not able to re-charge. Energy becomes a crucial issue because of the dynamic changes in sensor nodes behavior in terms of bandwidth, distance, mobility and so on. The Quality of Service is decreased due to certain problem on top of topology control, way of communication among the nodes and access of the service[11]. It includes route discovery, neighbor selection, position identification and radio transmission distance. Some of the data communication problems are routing, broadcasting, multicasting, geo-casting and location updating.

Nowadays WMAN are used often to carry confidential information in certain applications like military and Government applications of WMAN. One of the crucial requirements in the above kind of network applications is security. Since security is a major portion of the WMAN, it must be considered forever during data transmission. This type of environment needs to provide a secured platform to transmit a data in a confidential manner.

One of the most key methods applied to reduce the power consumption is clustering. Most popular methods such as PEGASIS[12], TEEN[13], LEACH[14], SER[15], HEED[16,17] and etc. are focused to save the energy in WSN. To understand the problem statement of this paper some of the existing approaches are discussed here. Mean field game theory[18] is proposed to MANET in order to provide security. But mean field game theory cannot attain multiple attackers and defenders at the same time. In[19] modified and extended the LEACH protocol to increase the network life time. The modified LEACH protocol is experimented in FAF-EBR [Forward Aware Factor-Energy Balanced Routing] method, where it can be applied only for industrial application under WSN. One of the authors in[20], brought topological based changes, coordinates based changes for authentication purpose. Using the topological structure the functionality of the network applications can be identified. In[21] the author used a recursive least square algorithm combined with reduced complexity for increasing the throughput of the network in all kind of distributed networks. Amplify-and-Forward method was proposed by[22] for data transmission where the data error, energy consumption among the sender and receiver are rectified and reduced respectively. Whereas the existing energy efficient protocols, mechanisms are not satisfied the user in terms of security. This paper proposed a secured clustering approach where energy efficiency with security is provided by integrating security mechanism and clustering approach together. The security is given in terms of examining nodes, timing and other relevant information collected during data transmission. In the existing research[6], the author discussed and proposed Defending against DoS (DAD) where DAD works in all the ways to detect and prevent DOS attack. Identity verification, Static IP assignment verification and Auth-key based communication and packet monitoring with time stamp and IP. But WDT-CH approach improves the efficiency of MANET in terms security and improved QoS.

2. Problem Statement

Given a network G is defined as **N X N** is deployed with M number of nodes randomly. At initial level all nodes energy is assigned to the maximum limit. In the network base station is considered as a sink node or receiver. The entire nodes are deployed in the form of clusters, where each cluster is assigned with a Cluster Head. The Cluster Head is also behaved as a timer called "Watch Dog Timer (WDT-CH)-Cluster Head" and it is used to trace the health status of all other nodes. WDT-CH-CH is authorized by the base station. The unit of this timer is based on number of nodes deployed in each cluster. There are four types of modes are identified throughout the network operations called active, idle, sleep and non-active mode. In a specific time of intervals all nodes in the network is supposed to get active and sends the positive message to WDT-CH-CH. If any node fails to send the message packet to the timer node that node is considered non-active and it is isolated from the network by by-passing the node during path discovery or any other means.

Similarly, the WDT-CH-CH nodes in the network (G) will send the message to base station to ensure its identity like the other nodes. Most of the non-operational time all the nodes are in sleep mode which get wakeup by active message or the time interval whichever comes earlier. There is one more isolated mode called idle mode, which is to pause the current operation exist in the path for the specific period of time. Difference between sleep and idle mode is sleep mode will switch off the radio transceiver off and it does not allow any communication until it gets wake up by other node. Whereas, idle mode temporarily called off communication until the specified time expires. Here, routing tree is formed when data communication is considered among the network in two different ways. One is, node-to-Cluster Head and Cluster Head-to-Sink the second is that there is no ambiguity exists in the path from source to sink node. Because of cluster creation of nodes, the path will be formed based on the certain characteristics like density of the nodes, centric approach and bandwidth efficiency etc. But in general the cluster nodes communicated with the WDT-CH and WDT-CH communicates with BS (sink). The first method of communication is well known. Since the second method of communication is proposed in this paper, it is discussed to understand the whole concept of the proposed approach clearly.

An open path is considered here where no other nodes will be repeated in the unique communication line. The WDT-CH node takes care of health check called status word of all the nodes deployed in the region specified in specific time called 32 milliseconds. The nodes which are in the path say P will be active throughout the communication. The algorithm runs if AND'ed signal of all the nodes in the path should be active. Because of the modes specified node energy is utilized in a very least manner compare to earlier approaches. During sleep mode, no operation is carried out until active or link message to WDT-CH arrives. The message packet which is transmitted from source to sink is encrypted and decrypted and it is controlled by key distribution management. This key distribution is operated by the WDT-CH nodes in the network. The nearest WDT-CH node for the path initially distributes public key to the nodes in the path. Based on routing table the next hop node is identified and previous node called source node where data packets resides will ask key from WDT-CH node. Now WDT-CH node check for the updated status word for the destined node and sends key to the source node and one key to next hop node. The same operation follows until message packet or data packet reaches sink node. During this operation if any node fails to transmit the encrypted message packet to the next hop node within the specific time the expected node sends negative acknowledgement to WDT-CH node. In this case, WDT-CH node resend from the previous node by providing different key for message packet. The data packet is collected from the source and encryption done in WDT-CH side and transmitted directly to the next hop node where data transmission resumes. By this security is ensured in an esteem level to avoid data leak from the message packet because authorized nodes are participating in the communication and it is monitored by a special monitor node called WDT-CH node.

3. Network Model

A restricted amount of nodes are deployed in the network as cluster wise. Each cluster comprises M number of nodes where M ranges from 1 to 15. Each cluster has minimum of one to maximum of three WDT-CH nodes for improving the security and node status monitoring. Base station is considered as a sink node in which for all paths the sink node is the destination node and it is depicted in Figure 1. Initially all nodes are assigned with Node-ID, initial Energy as 100, location (x, y) and cluster-ID. Each Node-ID is clubbed with cluster-ID belongs to the corresponding cluster where the node is placed. Here maximum number of cluster is restricted to 4. Based on this cluster number nodes are identified. At every sample interval each node in the cluster sends its own status word to the selected WDT-CH node. Actually WDT-CH node is considered Main and Redundant. If anyone WDT-CH node fails in the network, spare WDT-CH node will be considered for loop. Hence redundant WDT-CH nodes are kept spare for the cluster in the network. The selected WDT-CH node receives the status word from all the nodes assigned in the cluster and updates the same to base station in case if any node is fault or fails.

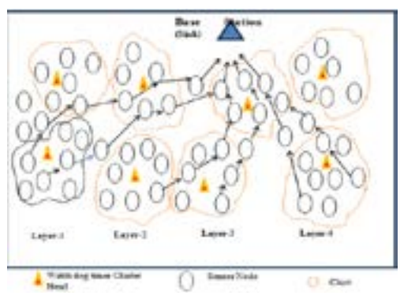

Figure 1. Proposed network model.

In the existing clustering approaches the cluster nodes transmits data to CH, the CH transmits the gathered data to BS directly or through other nearest CH to BS.

To ensure the data correctness if status word continuously received from the particular node by stating fail mode for 3 times, then only corresponding node is considered for removal and detach from network. This 3 time's check is to ensure the node failure for considerable time. One counter will be run if fail status of node is identified for first time for the corresponding node. If it crossed three then it reset the counter to zero and make that node as a fault node and provide the status to base station stating that not to consider the node for furthermore. The status word is depicted in Figure 2. The status word transmission is depicted in Figure 3. The nodes which belong to WDT-CH node in that cluster, specifies how node is transmitting the status word to it.

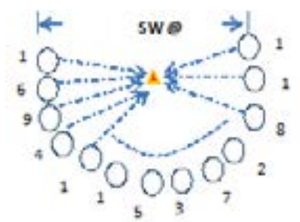

Figure 2. WDT-CH Node interaction with sensor nodes.

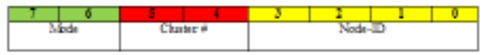

Figure 3. Status word header format.

Example, consider the bit pattern 11011100 is received by WDT-CHN$_2$ as an update from node 12 at time t_0. From this pattern LSB four bits specifies the node-ID, here 1100 called node-ID is 12. And fourth and fifth bit represents the cluster number; here 01 represents node-12 belongs to cluster-2. And MSB two bits represent the state of mode, here 11 represents the node-12 is active and health status is OK.

In other case if WDT-CH node receives the bit pattern 00111010 then according to the logic by extracting the MSB two bits, it clearly tells that the node is in non-active mode. In this case WDT-CH will not assign the node as a fault node in very first case. Instead one up counter is triggered from WDT-CH side to keep track the same pattern received from the node-5 in next update. If counter reaches 3, then WDT-CH treat the node-5 as a faulty node. The bit pattern and the corresponding mode are depicted in Table-1.

Table 1. Bit pattern for mode and cluster selection for status word

Bit Pattern	Mode	Cluster
00	Non-Active / Not-OK	Cluster-1
01	Idle	Cluster-2
10	Sleep	Cluster-3
11	Active /OK	Cluster-4

Idle and sleep mode in the received pattern is generally don't care bits because both patterns are set in communication. If number of nodes increases in clusters or number of clusters are increases above four then bit pattern size will vary up to 16 bits.

- Lemma-1:

Consider the CH set = $\{WDTCH_i \ldots DTCH_j\}$ is a set of link timer for the given network at an interval span of time. It updates the communication link to master sink or base station is depicted in Figure 4.

$WDTCH_i \in \{N_1, N_4, \ldots, N_i\}$

$WDTCH_j \in \{N_2, N_3, \ldots, N_j\}$

$WDTCH_i \bigotimes WDTCH_j \in N_c$

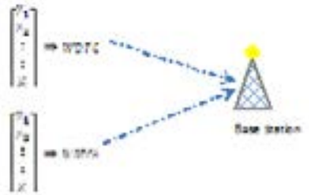

Figure 4. Watch dog timer node updating status to base station at time t_i.

- Lemma-2:

If node $n_1, n_2, \ldots, n_m \in Cluster_1$ and (WDTCH$_1$, ..., WDTCH$_n$, S$_N$) $\in$ N$_2$(then $Cluster_1 \cup Cluster_2 \in N$, and $Cluster_1 \cap Cluster_2 = \emptyset$. Node and timer nodes are always mutually exclusive.

- Theorem-1:

Let 'G' be a regular graph. Then there exists a sub graph G' which depends on G, Such that every node 'ω' in G such {[W] ≥ G', we can break ω in to:

i. $\propto \neq \in (or) |\propto| > 0 \ (or) |\propto| \geq 1$

ii. $|\propto \beta| \leq G'$

iii. for all j ≥ 0, the graph node $\propto \beta^j \times z$ is also in graph G.

- Theorem-2:

Prove that $G = \{\alpha^n | n = i^z, i \geq 1\}$ (or) $G = \{\alpha^n | n = i^z, i \geq 1\}$is not complete note in network G.

- Solution:

Assume graph 'G' in a network. Numbers of nodes are $G = \{\alpha^n | n = i^z, i \geq 1\}$. Number of node is n. Take any path '**ω', let ω=**α^n where n is called i^z, then the length of the path is **| ω| = n.**

|ω| ≥ n, we can split into

$\omega = \alpha^n . \omega = (\textbf{path nodes}) Cluster_1 \times Cluster_2 \times Cluster_3 .$

$\propto \beta = \alpha^n$

$\beta = \alpha^j$

$\gamma = \alpha^{n-m}$

$|\propto \beta| \leq n$

$|a^n| = m \leq n$

$\propto \beta^k \cdot \gamma = \alpha^m (\alpha^j)^{k-1} \alpha^{n-m}$

If apply k = 0, 1, 2 that doesn't belongs to graph G.

- Algorithm:

//Watch dog timer node chk.
//Specification: WDT-CH timer is a network node which keeps track the status word of all the assigned nodes in the cluster for health check in Equal intervals.
// Input: Network G within valid nodes.
// Precondition: All nodes are assigned with a new energy level and authorized by BS.
// Exit criteria: All assigned nodes health check receive 0.

- **Algorithm-1: WDT-CH_chk_Node ( )**

Begin:

i. G = (Cluster$_1$, Cluster$_2$, … ,Cluster$_m$) // valid graph G with N nodes and m clusters

ii. WDT-CHN = subset of G (or) G' where G' is the sub graph of G.
G' = $\{Cluster_1, Cluster_2, \ldots, Cluster_i\}$
(i.e.) G'$\cap G = G'$.

iii. WDT-CHN $\in G \in G$ network.

iv. At time $T_0, T_{t+1}, T_{t+2}, \ldots$
WDT-CH$\xrightarrow{statusword}$ BS
TC = $T_0, T_{t+1}, \ldots$.

v. for I = 1 to Node-n and time T_t
loop
node (Cluster$_i$)$\xrightarrow{statusword}$WDT-CHN
end loop

vi. extract MSB 2 bits from SW and check for active mode.
if active
health (node) = OK
else
increment-counter, if counter > 3 node = non-active / dead
counter =0
end if

vii. Extract 4 bits from LSB of SW and obtain node ID, Cluster where the node belongs is extracted by 3rd and 4th bits of the SW.

viii. WDT-CH updates the status table for the nodes in the region.
If health (node) is not OK,
remove node from network assign route discovery update network
else
do Null
end if

endWDT-CH_chk_node.

- **Algorithm-2:Path_Routing_Tree**

// input: Network G with n authorized nodes, Clustered node deployment by Sink node.
//Precondition: Active status of WDT-CH node in clustered network.
// exit Criteria: Path P found.
Path_Routing_tree.
Begin.
Ti <- Empty Tree.
Pi <- Path {0}.
ActFlg<- ActiveState (Node$_i$<<and>>Node$_j$<<and>> :: Node$_x$).

- **Procedure Active Begin then**

If ActFlgi then
Ti <- link(ni)
ni: = next_hop_routing table(i)
return i
else
do nothing
end if
end procedure Active
for node$_i \neq \emptyset$ loop

call Active;
end loop
return (Ti <- Pi)
end Path_ Routing_Tree

- **Algorithm-3: Data Packet Transmission**

// Input: 1. Path P, 2. Constructed routing tree for path P.
// Precondition: Path P and Tree Ti is set.
// Exit Criteria: If data packet received by sink or Transmission called off.
Data Pkt_Tx_SrcToSnk.
Begin
node<- Pi
next_hop Pi+1
{ $Cluster_1$, $Cluster_2$,…., $Cluster_i \in P$ } <- $WDT\text{-}CH_k$
Loop Cluster1,,..Clusteri $\in P$ then
WDT-CH<-nexthop($Cluster_i$)
($Cluster_i \in P$) <-$WDT\text{-}CH_{new\_key}$
Data <- encryption_pkt(data)
(Node ($Cluster_i$) $\in P$) <- Data
if node state fails
WDT-CH<- $n_i(-1)$
restart for node n_i
next_hop<- P_{i-1}
$WDT\text{-}CH_{data}$<- SinkNode(Data)
node(n_i)data <- $WDT\text{-}CH_{data}$
end if
clears data pkt from $WDT\text{-}CH_{data}$
$Path_p$<- 0
$WDT\text{-}CH_p$<-
RoutingTreeT<-
end DataPkt_Tx_SrcToSnk

The above algorithm has three partitions called steps, they are:

- Watch Dog Timer Based Node Check.
- Path Routing Tree.
- Secured Data Transmission.

WDT-CH based node check is a network node which keeps track the status word of all the assigned nodes in each cluster for derive the health check. There is main and redundant WDT-CH nodes are identified in each cluster to monitor the other sensor nodes in the region. The same is described in Algorithm 1. Consider the network with randomly deployed nodes maximum 4 clusters it will be partitioned. Each sub clusters is organized by WDT-CH node. At specific time intervals all the nodes in the cluster transfers the status word packet to the selected WDT-CH node for loop. From the status word state of the node is derived with health check and the same is passed to the base station. BS keeps trace of node by status word specification. Status table is maintained if any node information in future requires about the nodes the recent status word details is in this status table. It ensures the recent health check of the nodes participated in the network. If health check is affirmative then the nodes are in good condition to support data communication, whereas if health check is not affirmative then from WDT-CH side one counter is assigned to ensure the same health check for 3 time, after 3 count the same status remains from the node, then the node which health is not affirmative is removed from the network. The same is intimated to BS. For future communication or path discovery the node will not be considered.

In path routing tree, the path nodes are connected without ambiguity to the destined node. A path which is considered for communication is done after the collective AND check of all the nodes in the path. Active flag is used in software side reads the active status from the sensor nodes in the path. If this flag is set then based on the route, routing table is updated with next hop nodes. The same step is followed until all the nodes in the path are considered for routing table update. Finally routing tree is formed based on the valid path and ready for transmission.

Data transmission is starts from the source node by holding the data packet and passed to the authorized node in the path by routing table next hop. Here key distribution scheme is handled by WDT-CH node. Initially WDT-CH node will send key to path nodes for ensuring the communication. Based on the next hop the current node knows the next node and request WDT-CH to pass the data packet to next node. WDT-CH is now assigns two keys one to current node and one to target node. With that encryption happens in current node, the key which sent to target node is used for accepting the data packet. It will not decrypt to identify data; here for acceptance of data packet key is used, the general data is encrypted in initial node. Individual encryption and decryption is to check whether valid nodes in the path are used for communication. With the help of WDT-CH node key is received by both the ends of data transmission tag. If decryption fails or any failures like data packet loss during transmission, WDT-CH node declares transmission failure. This WDT-CH node knows the tag nodes will rise for a key in the stipulated time. If no key requirement triggered from tag end, it declares the failure. In this case, WDT-CH node receives the data packet from the source node and delivers to next hop node where data transmission paused. Then continuity of process is same like proposed method until sink receives the data. After successful completion of data transmission path is cleared and tree is available for next dynamic update.

3.1 Routing Tree

An unambiguous tree structure is formed by linking path nodes from source to sink node which is called BS. Parent child links is established for packets forward. High efficient bandwidth and energy is utilized for data communication. A node receives the data packet based on the next hop link and in the order of tree structure, a set of protocols and rules are certain to the MAC cluster of node, with the help of WDT-CH node it passes to the other node in an efficient way by secured encryption methods. The tree structure is depicted in Figure 5. The path metrics in the tree obtained is calculated by as follows:

Path Metric in routing tree:

$$M_p = \frac{(\text{No. of Hops for Path} * \text{Max. load in path})}{Probabilty of Path Success}$$

The structure consists of flow control mechanism which acknowledges for every node communication. The proposed approach is comparatively studied with earlier approaches like secured energy efficient mechanism. Parametric like throughput is considered, where successful delivery of message is achieved for every communication. The efficacy of the routing tree mechanism is high due to clustering based tree conversion.

Figure 5. Routing tree structure with sink node including clustering.

4. Simulation Settings

The proposed schemes have been experimented in the simulation environment in ns2. The simulation parameters are shown in Table 2.

The network deployed with 60 nodes, where 15 nodes per cluster and maximum of four clusters in the network can accommodate this 60 nodes along with WDT-CH nodes. During the communication the proposed approach functionality is verified and investigates how this approach is efficient in terms of saving the energy and detecting malicious nodes in the network. The simulation results are shown in the following figures and discussed in following section.

Table 2. Simulation parameters

Parameter	Level
Area	1500m x 1500m
Speed	1 to 25 m/s
Radio Propagation Model	Two-ray ground reflection
Radio Range	250 m to 300 m
Number of Nodes	15 per cluster and 4 clusters
MAC	802.11x
Application	CBR, 100 to 500
Packet size	50 and above
Simulation Time	50s to 100 s
Placement	Random Deployment
Malicious Population	Up to 5%
Common malicious node	5%
Pause Time	5ms

5. Results and Discussion

The simulation network taken considerable nodes to pass the algorithm, based on the output the basic metrics like throughput, Packet Delivery Ratio (PDR), End-End Delay, Residual energy is calculated and the same is compared with earlier approach. Time with delay is compared and shown in Figure 6. Time is considered in seconds and delay is verified with the data transmit of packets from source and receiver of destination. Each level of iteration the node communication is estimated with transmission time and node delay. In existing approach delay obtained is maximum level where time increases. Using WDT-CH nodes here the delay is qualified in transmission stage from one node to the other. If node fails to trigger for data transmission within the specified time, WDT-CH will take care of further process, hence delay is handled optimistic.

Figure 7 depicts the comparison of Packet Delivery Ratio between existing and proposed approach. Number of nodes considered here in terms of 10 to 70, each time the probability of successive PDR obtained is calculated as follows:

$$PDR = \frac{\#\ PacketsReceived}{\#\ PacketsTransmitted}$$

For the approximate time within the specified range, how many packets are received by the sink node is given in the Figure 7. It clearly states that for proposed approach PDR is high that is for maximum number of packets transmitted, all packets which is controlled by WDT-CH node is received by the sink node.

In this proposed approach, main goal is how to use energy efficiently when sensor node really not in use. For this several modes is identified in proposed system, each node usage and activities is clearly handles the anomalies in energy efficiency. It is depicted in Figure 8, number of nodes is compared with energy levels. Node is considered in all cluster levels as per the network model. All nodes are in different modes, mostly in sleep mode except path nodes in action or node busy in sending status word. This approach is compared with existing system; the proposed model defines efficient energy usage between the nodes.

Since this proposed approach follows clustering technique, the efficacy of the energy saving is verified in the simulation. To do this, the simulation is carried out five rounds where in each round the number of nodes deployed is varied. In all the five rounds there are 200 number of nodes in increased from round one to round five. After each round the remaining energy of the cluster nodes are calculated and verified. According to the data size, distance among the nodes and the Cluster Head, Cluster Head to BS the energy consumption is changed. When the amount of energy (battery level) goes below a lowest threshold value the node become a dead node. And the dead node can be activated after providing full battery charge or replacing the battery. In this paper the number of dead node ratio proportionally increased by 2.5% than the previous level. Hence this proposed approach is efficient in terms of monitoring, acknowledging, energy efficiency and throughput and shown in the Figure 6 to Figure 9.

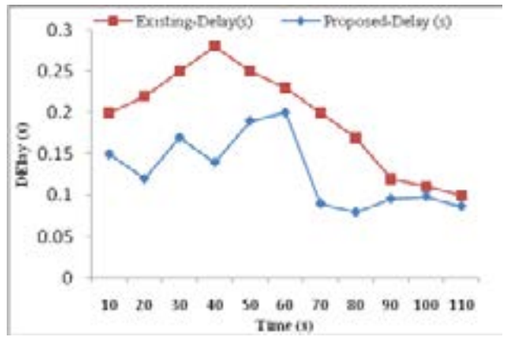

Figure 6. Delay comparison between existing and proposed approach.

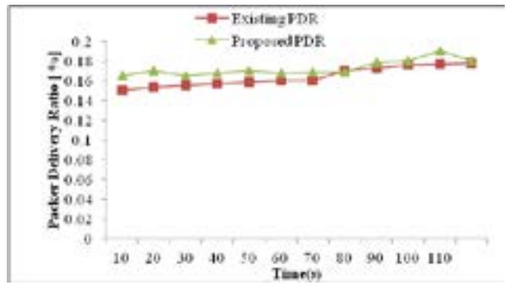

Figure 7. PDR comparison between existing and proposed approach.

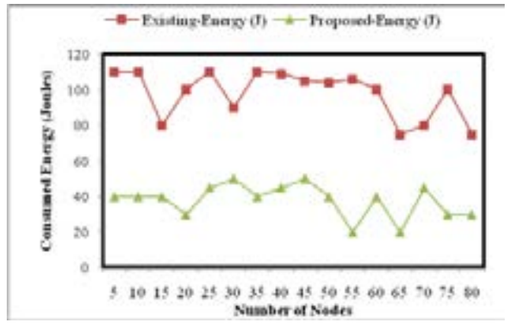

Figure 8. Energy comparison between existing and proposed approach.

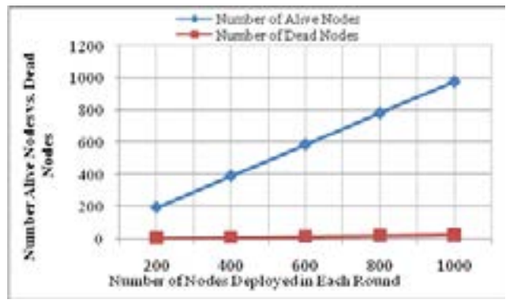

Figure 9. Clustering efficiency.

6. Conclusion

The main objective of the paper is to reduce the energy consumption among the nodes and improving the security. To do this WDT-CH node based monitoring the nodes health status to communicate efficiently. Here, WDT-CH node is acting as a Cluster Head as well as monitoring node in the clusters and since it is efficient to provide security and energy efficient in the network. This secured clustering leads to prevent data loss and reduce the delay while routing. From the simulation results it is clear and concluded that the proposed WDT-CH approach is efficient mechanism for improving secured energy efficient network.

In future, if the status word size increases, network size also increase with more number of nodes. Over to this, WDT-CH node for each cluster main and redundant is used here, if any one WDT-CH sensor node fails, the other one is considered for a loop. If number of nodes increases, clusters in the network also increases. Hence, WDT-CH shall be selected based on centric access to the cluster nodes. By this proposed model, energy level is consumed up to the maximum consumption using different mode specified and security is implemented throughout the communication.

7. References

1. Kokilamani M, Karthikeyan E. A novel technique to control congestion and energy aware routing scheme for Wireless Mobile Ad hoc Networks. Indian Journal of Science and Technology. 2016 Jul; 9(26):1–11.
2. Ramalingam M, Isa NAM. Video steganography based on integer Haar wavelet transforms for secured data transfer. Indian Journal of Science and Technology. 2014 Jan; 7(7):1–8.
3. Ashok J, Thirumoorthy P. Design considerations for implementing an optimal battery management system of a Wireless Sensor Node. Indian Journal of Science and Technology. 2014 Jan; 7(9):1–5.
4. Mishra A, Singh SS, Bhattacharya S, Pattnaik PK. A novel area coverage management scheme for sensor network with Mobile Sensor Nodes. Indian Journal of Science and Technology. 2012 Aug; 5(7):1–6.
5. Micea MV, Stancovici A, Chiciudean D, Filote C. Indoor inter-robot distance measurement in collaborative systems. Advances in Electrical and Computer Engineering. 2010; 10:21–6.
6. Roy ATP, Balasubadra K. DAD: A secured routing protocol for detecting and preventing denial-of-service in Wireless Networks. Wireless Personal Communications: Springer; 2015 Aug. p. 1–15.
7. Filograno ML, Guillen PC, Barrios AR, Lopez SM, Plaza MR, Alguacil AA, Herraez MG. Real-time monitoring of railway traffic using fiber Bragg grating sensors. IEEE Sensors Journal. 2012; 12:85–92.
8. Li J, Jia QS, Guan X, Chen X. Tracking a moving object via a sensor network with a partial information broadcasting scheme. Information Sciences. 2011; 181:4733–53.
9. Kwon T, Hong J. Secure and efficient broadcast authentication in Wireless Mobile Ad-Hoc Networks. IEEE Transaction on Computers. 2010; 59:1120–33.
10. Fernandez I, Asensio A, Gutierrez I, Garcia J, Rebollo I, No JD. Study of the communication distance of a MEMS pressure sensor integrated in a RFID Passive Tag. Advances in Electrical and Computer Engineering. 2012; 12:15–8.
11. Jung SJ, Kwon TH, Chung WY. A new approach to design ambient sensor network for real time healthcare monitoring system. IEEE Sensors; Christchurch. 2009. p. 576–80.
12. Gokce EI, Shrivastava AK, Cho JJ, Ding Y. Decision fusion from heterogeneous sensors in surveillance sensor systems. IEEE Transaction Automation Science and Engineering. 2011; 8:228–33.
13. Huang G, Li X, He J. Energy-efficiency analysis of cluster based routing protocols in Wireless Sensor Networks. IEEE Aerospace Conference; 2006. p. 1–8.
14. Akkaya L, Younis M. A survey of routing protocols in Wireless Sensor Networks. The Elsevier Ad Hoc Network Journal. 2005; 3(3):325–49.
15. Lindsey S, Ragavendra C. PEGASIS: Power Efficient Gathering in Sensor Information Systems. IEEE Aerospace Conference Proceedings. 2002; 3(9-16):1125–30.
16. Fu C, Jiang Z, Wei W, Ang WEI. An energy balanced algorithm of LEACH protocol in WSN. IJCSI. 2013 Jan; 10(1):354–9.
17. Su W, Akyildiz IF. A Stream Enabled Routing (SER) protocol for Sensor Networks. Med-hoc-Net 2002; Sardegna, Italy. 2002 Sept. p. 1–20.
18. Kour H, Sharma AK. Hybrid energy efficient distributed protocol for heterogeneous Wireless Sensor Network. International Journal of Computer Applications. 2010; 4(6):1–5.
19. Wang Y, Yu FR, Tang H, Huang M. A mean field game theoretic approach for security enhancements in Mobile Ad hoc

Networks. IEEE Transactions. 2014; 13(3):1616–27.
20. Zhang D, Li G, Zheng K, Ming X, Pan ZH. An energy-balanced routing method based on forward-aware factor for Wireless Sensor Networks. IEEE Transactions. 2014 Mar; 10(1):766–73.
21. Dhanapala DC, Jayasumana AP. Topology preserving maps - Extracting layout maps of Wireless Sensor Networks from virtual coordinates. IEEE/ACM Transactions. 2014 Jun; 22(3):784–97.
22. Liu Z, Liu Y, Li C. Distributed sparse recursive least-squares over networks. IEEE Transactions. 2014 Jan; 62(6):1386–95.