Research Journal of Applied Sciences, Engineering and Technology 7(17): 3458-3465, 2014
DOI:10.19026/rjaset.7.697
ISSN: 2040-7459; e-ISSN: 2040-7467

Submitted: September 09, 2013 Accepted: November 11, 2013 Published: May 05, 2014

Research Article

Cluster Based Failure Detection and Recovery Technique for Wireless Body Area Networks

K.T. Meena Abarna and K. Venkatachalapathy
Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, India

Abstract: In Wireless Body Area Networks (WBANs), the extremely sensitive data transmission mainly requires fault tolerance and consistent data transmission. In this study, we propose a Cluster Based Failure Detection and Recovery Technique for WBAN which presents a hierarchical architecture. Here, local nodes are connected to their Cluster Heads (CHs). Each CH is interconnected and also connected with a Wireless Local Gateway (WLG). Finally, WLG is connected to Hospital Gateway (HG). Each local sensor collects the fault related information and each node is assigned with priority to measure the fault tolerant level of individual nodes. Nodes with high priority are processed first. Further, node and CH level faulty node detection and recovery schemes are also proposed. Our technique provides both reliability and fault tolerance. The efficiency of our technique is proved through simulation results.

Keywords: Cluster heads, hospital gateway, wireless body area networks, wireless local gateway

INTRODUCTION

Wireless Body Area Networks (WBANs): Wireless Body Area Network (WBANs) can be termed as a distributed system, where nodes are distributed on the human (patient) body. The deployed sensors are utilized to sense some physical quantities in human body such as heart beat rate and body temperature. The sensed data are transmitted to the central device and then forwarded to a remote place making use of sink node (Ali, 2010). As a result of supporting information infrastructure, WBAN has unmatched opportunities in health care systems (Warren *et al*., 2005). At first, BAN was introduced to get along with personal consumer electronic devices. However, later telemedicine and m-health applications necessitate and used BAN at various parts of human, who need prolonged treatment (Poon *et al*., 2006).

In BSN, sensors are distributed in a patient's body and interconnected with each other. The interconnected sensors are attached to a microprocessor. In general a BSN node encompass of a wireless transceiver and a battery. A range of wireless access technologies incorporate the outside environment (Bao *et al*., 2008; Sharifi and Alamuti, 2007).

Each BAN node processes biological data that are collected from various parts of human body. These information are collected at periodic intervals for monitoring and diagnosing patient's health systematically. As WBAN makes possible joint processing of biological data, it becomes a prominent research area (Bao *et al*., 2008). Commonly, wireless body area network is constructed using star topology. Thus, the processed data at sensor nodes are forwarded to the central processing node for processing and aggregating sensed data. As WBAN is used in human body, reliability of data is an important objective as human life (Ali, 2010).

WBANs are widely useful to monitor patients, when a physician is not available. Other than this, it is useful to in-hospital patients, people in Intensive Care Unit (ICU) when proper Radio Frequency (RF) technology is implemented (Bao *et al*., 2008). Low complexity nodes, limited transmission and processing power, high reliability, mobility, reduced latency and dispersive RF are some of the characteristics of WBAN that makes it inimitable from other networks (Arrobo and Gitlin, 2011).

Since, WBAN transmits lifesaving related information such as heartbeat rate transmission for heart attack; the transmitting data must be reliable. It must be capable of facilitating self-healing after failures like link failure. Nodes should be implemented with energy efficient technique to consume less energy. It should keep up with good throughput even under dynamic and challenging channel conditions (Arrobo and Gitlin, 2011).

Fault tolerance: In WBAN, both software and hardware failures significantly affects the behavior of

Corresponding Author: K.T. Meena Abarna, Department of Computer Science and Engineering, Faculty of Engineering and Technology, Annamalai University, India

nodes. Failure at particular region affects entire nodes belong to that transmission range. Communication fault can be categorized as hardware failure. This fault causes failure in the network due to energy depletion and it may also reasoned by environmental factors such as rain and wind (Gupta and Younis, 2003; Senoussi *et al*., 2012).

The process of communication in WBAN must be accomplished without any fault occurrence as it transmits extremely sensitive data that deals with health care applications. Achieving fault tolerance in WBAN is complicated owing to distinct networking situations (Yoo *et al*., 2009). The fault tolerant design technique in routing protocol of WBAN may wear out all resources easily and consequently leads to downfall of nodes (Santhosha and Sujatha, 2012).

The network capability of maintaining connectivity even after failures and attacks is termed as reliability. Maintaining reliability in wireless body networks is an important issue (Wang *et al*., 2009). WBAN must be skilled to get back from link and node failures. Further, WBAN must facilitate minimize data loss and bounded latency by providing robustness in the links. Finally, the fault tolerant technique must adapt dynamically with changing environment and user state (Reichman, 2009).

Problem identification: In our previous study, Meena Abarna and Venkatachalapathy (2012) we have proposed security architecture for body sensor networks. Here, we assume the existence of a Certificate Authority (CA) server situated in the hospital. The local sensor collects data from the patient's body and sends to the cluster head. WLG maintains a table and broadcasts it to the respective CHs. Each CH aggregates data from the local sensors and generates the message which is encrypted by Ksec at the CH and sent to the WLG.

At the WLG, the message is decrypted using the same key Ksec, to ensure the security of the data. Then a new message is created by aggregating all messages from various clusters of a patient. For each patient, a new string is generated and a public key Puk is created from the string using ECC. The string is then stored in the CA. The WLG then encrypts it and a MAC has been created for this, using the shared key between WLG and HG. The MAC value is transmitted to the HG. If the MAC value is matched with the already calculated MAC value, then the message is forwarded to the destination. At the destination, when the data is required by the authorized person, a request is sent to the CA. CA then generates the corresponding private key Prk for decryption.

The technique concentrates mainly on the security issues, but it does not deal with the failure that occurs during the extremely sensitive data communication since there is a chance for occurrence of fault at the sensor node and cluster head. Failures significantly affect the behavior of nodes and hence reducing the performance of the network. Therefore, failure detection is required. Once the failure is detected, recovery technique is used to find the solution.

To overcome these issues, in this study, we propose cluster based failure detection and recovery technique for wireless body area networks to our previous security architecture (Meena Abarna and Venkatachalapathy, 2012).

LITERATURE REVIEW

Gupta and Younis (2003) have proposed an efficient mechanism to recover sensors from a failed cluster. This approach avoids a full-scale re-clustering and does not require deployment of redundant gateways. They have investigated the dependability of sensor networks in the presence of faults in the gateways. Their mechanism is a run-time recovery mechanism based on consensus of healthy gateways to detect and handle faults in one faulty gateway. A two-phased detection and recovery mechanism is proposed to limit the performance impacts caused by a gateway failure. The drawback of this study is that they have not considered the movement of gateways.

Wu *et al*. (2010) have introduced an adaptive and flexible fault-tolerant communication scheme for BSNs called as AFTCS. When channel impairments occur, AFTCS can provide reliable data transmission for critical sensors by reserving channel bandwidth according to the perceived information about human physiological status, external environment and the system itself. Fault-tolerant priority and queue are employed to adaptively adjust the channel resource allocation.

Ould-Ahmed-Vall *et al*. (2011) have presented a general fault tolerant event detection scheme that allows nodes to detect erroneous local decisions based on the local decisions reported by their neighbors. This detection scheme does not assume homogeneity of sensor nodes and can handle cases where nodes have different accuracy levels. They have described two new error models that take into account the neighbor distance and the geographical distributions of the two decision quorums. Their models are particularly suitable for detection applications where the event under consideration is highly localized.

Raj *et al*. (2008) have proposed a fault tolerant and energy efficient clustering approach which organizes the whole network into smaller cluster and sub cluster groups enabling a considerable reduction of communication and processing overhead. Sub cluster formation also gives the possibility to skillfully deal with sensor nodes, node leader and cluster head failures. They have also proposed a fault tolerant approach that uses a matrix based error approximation

method for providing the approximate sensor data of the failed node.

Abolfazl *et al*. (2011) have designed techniques to maintain the cluster structure in the event of failures caused by energy-drained nodes. First, node with the maximum residual energy in a cluster becomes cluster heed and node with the second maximum residual energy becomes secondary cluster heed. Later on, selection of cluster heed and secondary cluster heed will be based on available residual energy.

MATERIALS AND METHODS

Overview: In this study, we propose a Cluster Based Failure Detection and Recovery Technique for Wireless Body Area Networks. During distribution of nodes in the network, sensor nodes form different clusters. The sensed data by local sensors are transmitted to Wireless Local Gateway (WLG) through Cluster Heads (CHs), which are then directly forwarded to Hospital Gateway (HG). Each local sensor periodically collects three types of information namely, bio information, ecological information and node information. These information are collectively called as fault related information. The collected F_{info} information are forwarded to their corresponding CHs. Each CH maintains a fault tolerant table (F-Table) to store F_{info} information. The CH compares F_{info} with three predefined threshold values namely $Th_{bio,}$ Th_{ec} and Th_{ni}. Based on comparison each node is assigned with priority value, node that has high priority value is processed first. Further, node and cluster level fault detection technique is also proposed. At node level, CH is responsible for discovering faulty node. The faulty CH is identified by other CH's in the network. CH that finds the faulty CH trigger fault recovery mechanism. Using recovery mechanism, all member nodes under fault CH are re-cluster themselves and elect new cluster head.

Network architecture: Our WBAN architecture encompasses of wearable local sensors deployed on various parts of the body, WLG is installed in patient's premises that collect patient's information from local sensors and HG is the destination that gathers patient information from WLG. HG commonly refers to nurse or doctor authorized to monitor the patient's health condition. During the deployment network, nodes form different clusters. Each cluster has a cluster head. The local sensor collects data from different parts of the body and transmits the data to their respective cluster head. Each cluster head communicates with a wireless local gateway. The WLG forwards the collected information to the remote HG. Cluster Formation is described at length in our previous study. The network architecture is given in Fig. 1 (Meena Abarna and Venkatachalapathy, 2012).

From network architecture diagram (Fig. 1), we can observe that CHs are interconnected. This CH interconnection is functioned to accomplish fault tolerant technique at CH level.

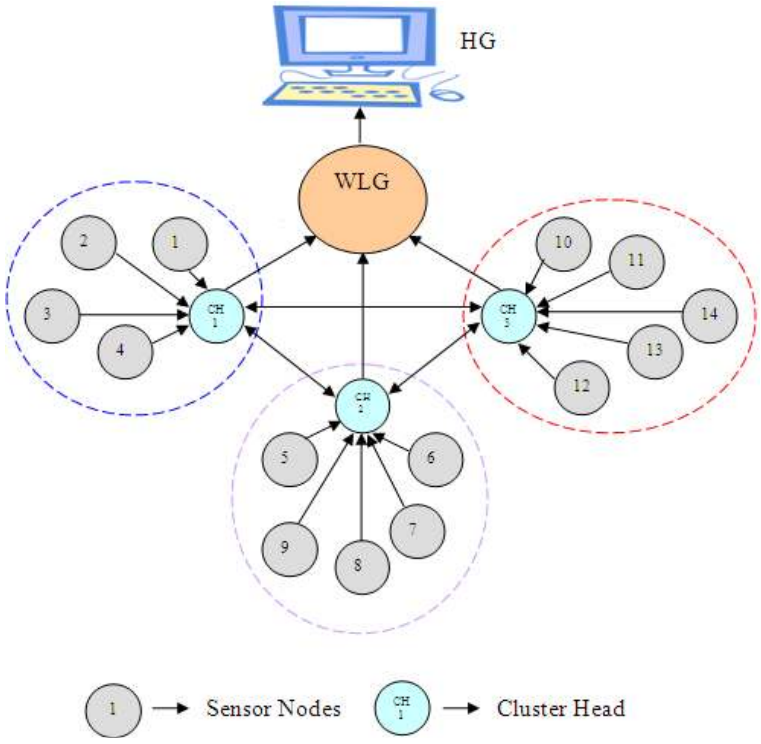

Fig. 1: Network architecture

Table 1: F_{info} message field format

Node ID	Cluster ID	Bio-info	Eco-info	Node info

Table 2: Format of F-table

Node ID	Fault related information			Priority degree
	Bio-info	Eco-info	Node info	

Priority based fault tolerant strategy: Consider BS_1, BS_2 … BS_n are the set of sensor nodes distributed in the human body. Each node periodically collects fault related information (F_{info}) and forwards to their respective CHs. F_{info} includes bio information, ecological information and node information. Bio information is physical and functional information of human being. Mostly, bio information is distinct to each man. Body temperature, heart rate and blood pressure are the typical examples of bio information. Ecological information is the environmental information around the patient such as room temperature, humidity and light. Node information is collected to identify the fault tolerant level of node current state. Since, sensor nodes have stringent energy and bandwidth resources, the residual energy and buffer usage are the significant parameters to evaluate the state of individual sensor node.

As, each BS has the ability to sense the information inside the patient and around the patient environment. It is possible to gather bio, eco and node information. At each time interval 't', each sensor node forwards F_{info} message to its corresponding CH_i. The F_{info} message has the following fields, (Table 1).

The F_{info} information is collected by each CH_i to provide fault tolerant by allocating appropriate priority to each node. While receiving F_{info} message from sensor nodes, each CH_i keep track this information in its F-table (Fault tolerant). A general model of F-Table is shown below in Table 2.

The CH assigns priority degree to a node considering F_{info} message of it. The derived bio-info, eco-info and node-info values are compared against three predefined threshold values namely Th_{bio}, Th_{ec} and Th_{ni}, respectively. The threshold values are different for different applications. In some cases it may differ from a patient to a patient.

Algorithm-1:

1. BS_i be the wearable body sensor, (i = 1, 2 … n) and CH_i is the cluster head
2. Consider I_{bio}, I_{eco} and I_{ni} as the bio information, eco information and node information respectively
3. Th_{bio}, Th_{ec} and Th_{ni} be the threshold values of bio-info, eco-info and node-info respectively
4. BS_i forwards F_{info} message to CH_i
5. CH_i retrieves I_{bio}, I_{eco} and I_{ni} values of CH_i
6. CH_i performs comparison
   (6.1) If ($I_{bio}>Th_{bio}$, && I_{eco}, $>Th_{ec}$ && $I_{ni}>Th_{ni}$) Then
   High Priority is assigned to a node
   (6.2) If ($I_{bio}>Th_{bio}$, && I_{eco}, $>Th_{ec}$ && $I_{ni}<Th_{ni}$) Then
   Moderate Priority is assigned to a node
   (6.3) If ($I_{bio}<Th_{bio}$, && $I_{eco}<Th_{ec}$ && $I_{ni}<Th_{ni}$) Then
   Lower Priority is assigned to a node
7. End if

During the distribution of nodes, each BS has default priority value. This value is dynamically updated using algorithm-1. The priority value assures the reliability of data to be transmitted. Based on priority assignment value, processes in the nodes are allocated. Low priority number has high priority and nodes that have high priority value are processes first.

Failure detection and recovery technique:

Node level failure detection and recovery: As we discussed in below section, each node periodically forwards F_{info} message to its CH. The CH keeps alive the F_{info} message information in its F-Table. When the CH does not receive F_{info} messages for two consecutive 't' intervals, then the node is decided as failed node. Instantly, the CH transmits failure information to the WLG, the failure information includes node ID and time when the node has stopped updating F_{info}. By receiving failure information, the WLG directly forwards to HG to precede appropriate repair or replacement. Last updated time information is added in failure table as the node process critical information (Heartbeat, temperature).

Cluster head level failure detection: From the network architecture diagram (Fig. 1), we can observe that CHs are interconnected with each other. As same as sensor nodes, each CH periodically forwards HELLO messages to other CH's in the network. The HELLO message of CH includes other CH ids and corresponding time stamp of finally received HELLO message. The HELLO message of neighboring CH is keep track by each CH.

When CH_i does not receive HELLO message from CH_{i+1} for a long time, then CH_i considers CH_{i+1} as faulty node. However, in many cases this response-less behavior of CH is reasoned by link failure between CH_i and CH_{i+1}. Thus, a CH cannot be justified as faulty node until any other CHs in the network is still able to communicate with it. To cope with this kind of situations, when CH_i does not receive HELLO message from CH_{i+1}, it sends failure information to other CHs in the network.

While receiving failure information, each CH looks its table to verify the time stamp of lastly received HELLO message from the corresponding cluster head. When the time stamp information of other CH matches,

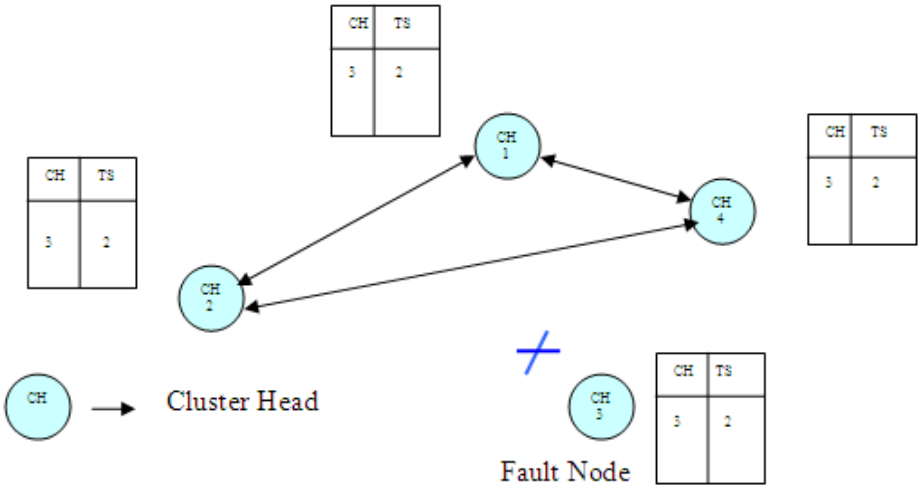

Fig. 2: Cluster head failure detection

then the node is declared as faulty and fault recovery mechanism is triggered.

Consider the scenario given in Fig. 2, CH1, CH2, CH3 and CH4 are cluster heads. All the CHs are interconnected. In that, CH2 finds that it does not receive HELLO message from CH3 for an interval 't_{CH}'. It sends failure information to all other cluster heads in the network namely CH1 and CH4. The failure information includes node ID and time stamp of last received HELLO message. While receiving failure information, CH1 and CH4 checks their tables for time stamp information. From Fig. 2, we can see that time stamp information of CH3 is same in CH1 and CH4. Thus, CH2 decides CH3 as fault node, it floods fault node information in the network and simultaneously triggers failure recovery mechanism.

Once the CH is failed, then the failure recovery mechanism has to recover all sensor nodes in that cluster. The CH that detects the failure of other CH invokes cluster head recovery mechanism. After the cluster head recovery mechanism is triggered, all cluster members under the fault cluster head are informed about CH failure. By receiving failure information, member nodes rearrange themselves and forms new cluster as described in our previous study (Meena Abarna and Venkatachalapathy, 2012).

Merits of our fault tolerant technique: Biological information, ecological information and node related information are collected to measure the fault tolerant level at each node and nodes are processed according to their priority values. Thus, our priority based fault tolerant technique measures fault tolerant level accurately and act accordingly, thereby it provides more than enough fault tolerance in the network.

Our technique reduces control overhead and energy consumption rate significantly as it minimizes the use more control signals.

The advantage of our proposed extension is that it is very robust because it provides fault tolerance for sensors and also clusters in the body area networks along with security as in our previous work.

RESULTS AND DISCUSSION

Simulation setup: The performance of the proposed Cluster Based Failure Detection and Recovery Technique (CBFDRT) for Wireless Body Area Networks is evaluated using NS2 (Network Simulator: http:///www.isi.edu/nsnam/ns) simulation. A network which is shown in Fig. 3 is deployed in an area of 50×50 m is considered. The IEEE 802.15.4 MAC layer is used for a reliable and single hop communication among the devices, providing access to the physical channel for all types of transmissions and appropriate security mechanisms. The IEEE 802.15.4 specification supports two PHY options based on Direct Sequence Spread Spectrum (DSSS), which allows the use of low-cost digital IC realizations. The PHY adopts the same basic frame structure for low-duty-cycle low-power operation, except that the two PHYs adopt different frequency bands: low-band (868/915 MHz) and high band (2.4 GHz). The PHY layer uses a common frame structure, containing a 32-bit preamble, a frame length.

The simulated traffic is exponential with UDP source and sink. Table 3 summarizes the simulation parameters used.

Performance metrics: The performance of CBFDRT is compared with the AFTCS (Wu *et al*., 2010) without applying the security scheme. The performance is evaluated mainly, according to the following metrics.

Average end-to-end delay: The end-to-end-delay is averaged over all surviving data packets from the sources to the destinations.

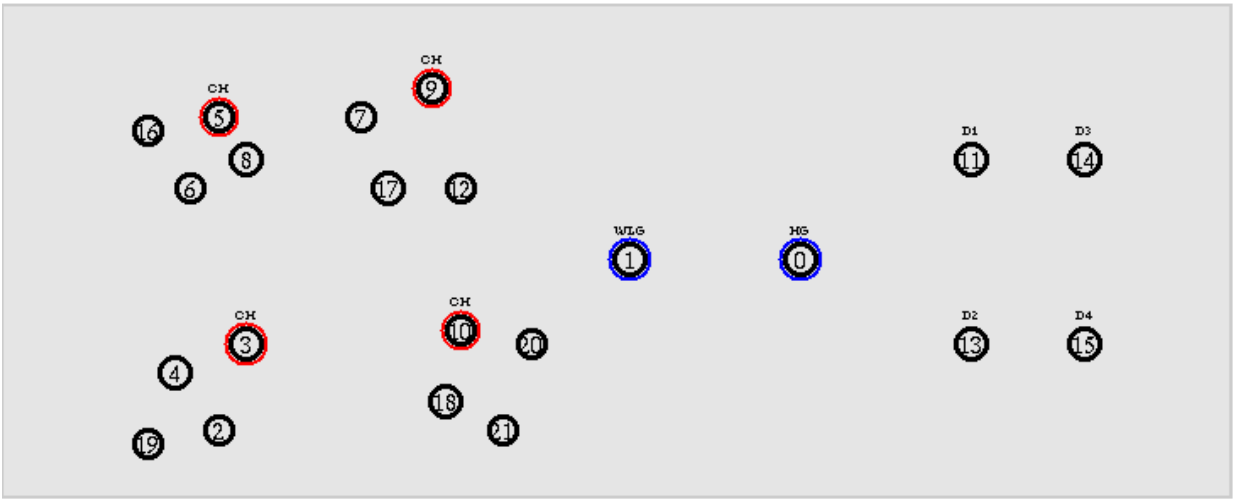

Fig. 3: Network topology

Table 3: Simulation parameters

No. of nodes	22
Area size	50×50
Mac	IEEE 802.15.4
Simulation time	25 sec
Transmission range	25 m
Routing protocol	LSA
Traffic source	Exponential
Rate	50 to 250

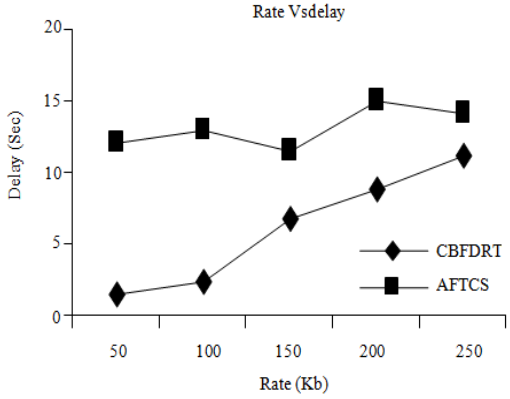

Fig. 4: Rate vs. delay

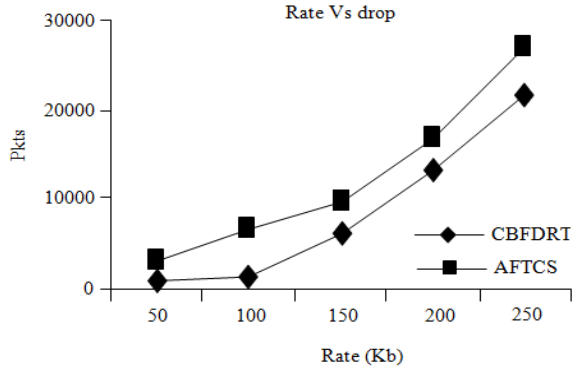

Fig. 5: Rate vs. drop

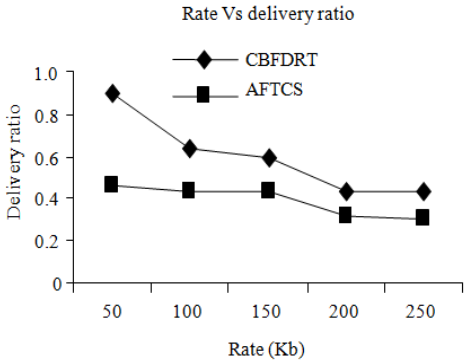

Fig. 6: Rate vs. delivery ratio

Average packet delivery ratio: It is the ratio of the number of packets received successfully and the total number of packets transmitted.

Packet drop: It is the number of packets dropped during the data transmission.
The simulation results are presented in the next section.

Results:
Based on rate: In the first experiment we vary the rate as 50, 100, 150, 200 and 250 kb, respectively.

From Fig. 4, we can see that the delay of our proposed CBFDRT is less than the existing AFTCS technique.

From Fig. 5, we can see that the packet drop of our proposed CBFDRT is less than the existing AFTCS technique.

From Fig. 6, we can see that the delivery ratio of our proposed CBFDRT is higher than the existing AFTCS method.

Based on packet size: In our second experiment we vary the packet size as 250, 500, 750 and 1000, respectively.

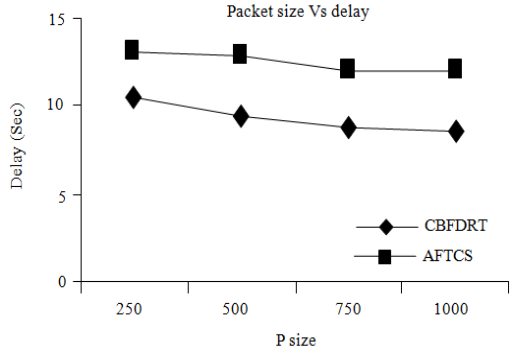

Fig. 7: Packet size vs. delay

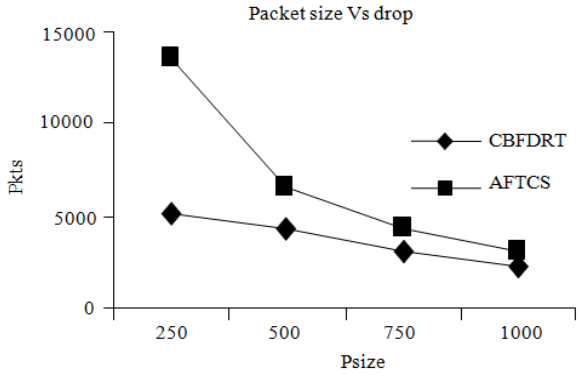

Fig. 8: Packet size vs. drop

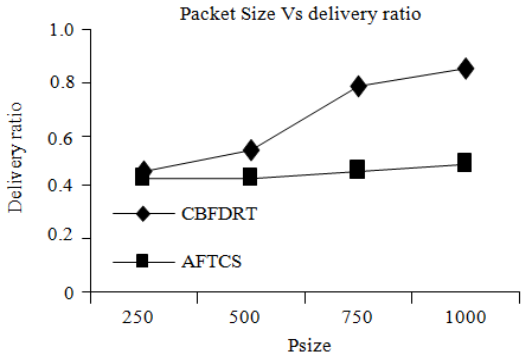

Fig. 9: Packet size vs. delivery ratio

From Fig. 7, we can see that the delay of our proposed CBFDRT is less than the existing AFTCS technique.

From Fig. 8, we can see that the packet drop of our proposed CBFDRT is less than the existing AFTCS technique.

From Fig. 9, we can see that the delivery ratio of our proposed CBFDRT is higher than the existing AFTCS method.

CONCLUSION

In this study, we have introduced a cluster based failure detection and recovery technique for wireless body area networks in which hierarchical architecture is used. Each local sensor collects fault related information and stores in a fault tolerant table. CH compares F_{info} with three predefined threshold values. Based on the comparison, each node is assigned with priority value to measure the fault tolerant level. Further, node-level and CH-level faulty node detection and recovery schemes are proposed. At node level, CH is responsible for discovering faulty node. The faulty CH is identified by other CH's in the network and the fault recovery mechanism is triggered. The efficiency of our technique has proved through simulation results. Our technique provides reliability and fault tolerance at hand.

REFERENCES

Abolfazl, A., D. Arash, K. Ahmad and B. Neda, 2011. Fault detection and recovery in wireless sensor network using clustering. Int. J. Wirel. Mob. Netw., 3(1).

Ali, P., 2010. Connectance and reliability computation of wireless body area networks using signal flow graphs. Life Sci. J., 7: 52-56.

Arrobo, G.E. and R.D. Gitlin, 2011. New approaches to reliable wireless body area networks. Proceeding of IEEE International Conference on Microwaves, Communications, Antennas and Electronics Systems (COMCAS), pp: 1-6.

Bao, S.D., C.C.Y. Poon, Y.T. Zhang and L.F. Shen, 2008. Using the timing information of heartbeats as an entity identifier to secure body sensor network. IEEE T. Inf. Technol. B., 12(6): 772-779.

Gupta, G. and M. Younis, 2003. Fault-tolerant clustering of wireless sensor networks. Proceeding of IEEE Wireless Communications and Networking (WCNC, 2003), 3: 1579-1584.

Meena Abarna, K.T. and K. Venkatachalapathy, 2012. Light-weight security architecture for IEEE 802.15.4 body area networks. Int. J. Comput. Appl., 47(22): 0975-8887.

Ould-Ahmed-Vall, E., B.H. Ferri and G.F. Riley, 2011. Distributed fault-tolerance for event detection using heterogeneous wireless sensor networks. IEEE T. Mobile Comput., 11(12): 1994-2007.

Poon, C.C.Y., Y.T. Zhang and S.D. Bao, 2006. A novel biometrics method to secure wireless body area sensor networks for telemedicine and m-health. IEEE Commun. Mag., 44(4): 73-81.

Raj, R., M.V. Ramesh and S. Kumar, 2008. Fault tolerant clustering approaches in wireless sensor network for landslide area monitoring. Proceedings of the 2008 International Conference on Wireless Networks (ICWN'08), 1: 107-113.

Reichman, A., 2009. Standardization of body area networks. Proceeding of IEEE International Conference on Microwaves, Communications, Antennas and Electronics Systems (COMCAS, 2009), pp: 1-4.

Santhosha, B.S. and B.R. Sujatha, 2012. Improving the quality of service in wireless body area networks using genetic algorithm. IOSR J. Eng., 2(6): 1291-1295.

Senoussi, C.M., B. Denaï. M. Zerhouni and A.H. Boudinar, 2012. A comparative study on feature selection to design reliable fault detection systems. Int. Rev. Comput. Software (IRECOS), 7(5): 2070-2077.

Sharifi, M. and A.N. Alamuti, 2007. A hybrid physical architecture for wireless sensor and actor networks. Int. Rev. Comput. Software (IRECOS), 2(5): 555-560.

Wang, S., J.W. Nah, K.J. Seok and J.T. Park, 2009. Analytical modeling of multi-type failures in wireless body area networks. Proceeding of IEEE International Conference on Broadband Network and Multimedia Technology (IC-BNMT '09), pp: 242-246.

Warren, S., J. Lebak, J. Yao, J. Creekmore, A. Milenkovic and E. Jovanov, 2005. Interoperability and security in wireless body area network infrastructures. Proceeding of 27th Annual International Conference of the Engineering in Medicine and Biology Society (IEEE-EMBS, 2005), 4: 3837-3840.

Wu, G., J. Ren, F. Xia and Z. Xu, 2010. An adaptive fault-tolerant communication scheme for body sensor networks. Sensors, 10: 9590-9608.

Yoo, J., S. Lee and H.J. Yoo, 2009. A 1.12 pJ/b inductive transceiver with a fault tolerant network switch for multi-layer wearable body area network applications. IEEE J. Solid-St. Circ., 44(11): 2999-3010.