International Journal of Engineering and Advanced Technology (IJEAT)
ISSN: 2249-8958 (Online), Volume-8 Issue-4, April 2019

Data Fault Detection Algorithm for Binary Sensor Networks

Vaishali S. Deshmukh, Arvind V. Deshpande, Parikshit N. Mahalle

Abstract*: Sensors are deployed in the real world to gather huge amounts of raw data. This unprocessed data contain meaningful information. However the data might not be correct due to faults in the sensors. So in order to draw valid conclusion, sensors producing faulty data need to be identified. This paper proposes an interesting approach to discover anomalous data from binary sensors. Our approach is able to differentiate correctly functioning and faulty sensors with respect to data fault. The correct interpretation of data is carried out by exploiting spatial and temporal correlations among sensor data. Experimentation shows that the proposed algorithm is able to identify faults in binary sensors. In various applications of sensor networks, the accuracy of sensor data directly affects the performance of that application. The proposed algorithm shows significant improvement in detection accuracy over existing technique for higher sensor fault probability.

***Index Terms*: wireless sensor network, data fault, binary sensor**

I. INTRODUCTION

Wireless sensor network applications deploy a large number of sensors to investigate a phenomenon occurring at the site. Sensors tiny size, low energy and communication need have increased its use in applications like event detection, habitat monitoring, home automation and control, environment monitoring, etc. These sensors over a period of time gather huge amounts of data. Several factors are considered while designing wireless sensor networks for an application. Major contributing things are scalability, fault tolerance and reliability. Commercial use of sensors in real time critical application scenario like fire detection is suffering a setback due to low reliability of data gathered by sensors. In practical implementations, faulty or abnormal sensor readings may be present owing to various unpredictable reasons such as harsh deployment environments, innately fault prone nature of sensors, aging. Faults in sensors may lead to degradation in system performance and moreover catastrophic situations. A sensor network was deployed to examine the microclimate over a large number of redwood trees. The cause of worry was presence of data anomalies. More than 50 percent data needed to be excluded as it does not serve any meaningful interpretation. Considering the critical nature of applications for which WSNs are perceived, the data collected by them should be unambiguous and reliable[1]. In order to improve sensor data reliability many different approaches are present in literature to filter out incorrect data. It is observed that a sizeable amount of data gathered by sensors is faulty. Four classes of methods are studied for fault detection: rule-based, estimation-based, time series analysis and learning based methods. Faults are modeled in three categories: short, noise, and constant. Rule-based methods require adjusting and tuning threshold parameter, learning methods are based on training phase, estimation methods cannot categorize faults, and time series analysis are found to exhibit highest rate of false positives[2]. Historical sensor data is modeled to find out faulty data and many of existing sensor fault detection methods are discussed Each future data instance is evaluated with respect to this standard[3]. This paper proposes a data fault detection algorithm to identify data faults occurring in the binary sensor network. The remainder of the paper is organized as follows: In Section 2, related work is discussed. Gap analysis of the related work is presented in Section 3. Section 4 presents a detailed working of binary sensors. Section 5 elaborates the data fault detection algorithm. Section 6 is about the result related discussion of the proposed algorithm. Section 7 concludes the presented work.

II. RELATED WORKS

An agnostic approach uses different parameters of a sensor node which are collected and examined to determine whether the sensor node is correctly working or faulty. The agnostic approach uses spatial and temporal analysis. In temporal method, it analyzes parameters of sensor node by pitching them against each other to draw gray scale images and draw conclusions. In spatial method, it analyses parameters of a sensor neighboring node and then draws gray scale images. A comparison of images of a sensor node with respect to its own is carried out with high computational complexity. Since it needs a large number of parameters to be observed, it is not feasible to be applied to binary sensors [4]. An anomalous node detection method consisting of training and detection phase can be used to detect faults. The training phase needs the data from all the sensors in the cluster. Further communication overhead is more as sensors in the cluster pass data [5]. Packet level attestation is a scheme for evaluation of data reliability in WSN. It makes use of the fact that typically nodes closer to each other exhibit similar data pattern.

Manuscript published on 30 April 2019.
***** Correspondence Author (s)
Vaishali S. Deshmukh, Department of Computer Engineering, Smt. Kashibai Navale College of Engg., Savitribai Phule Pune University, Pune, India..
Arvind V. Deshpande, Department of Computer Engineering, Smt. Kashibai Navale College of Engg., Savitribai Phule Pune University, Pune, India..
Parikshit N. Mahalle, Department of Computer Engineering, Smt. Kashibai Navale College of Engg., Savitribai Phule Pune University, Pune, India..

The data pattern may change over with time progress but two nearby placed nodes exhibit same data pattern. The algorithm uses a neighboring sensor node as data verifier node for each node. If the data of both the verifier node and sensor node is same then a bit is attached which signifies that the data is valid. The data of the verifier node itself needs to be authenticated as it may itself be faulty. A delayed attestation bit solution is proposed which needs to observe the data of verifier node for minimum 50 time cycles to validate using statistics. But in real time critical applications if the in network solution to verify data is time intensive then it is not feasible[6]. Certain methods aggregate the information received from neighbor sensors to identify anomalies amongst them. It is based on the idea that sensor readings of the sensors in close distance proximity tend to be similar. The amount of information extracted from the neighborhood and the size of the neighborhood are key aspects which characterize the correlation. The algorithm implementation results are affirmative when the data are well correlated. The proposed method is applicable to a set of applications monitoring natural phenomenon. The performance of the algorithm is evaluated using confusion matrix and other measures based on it [7]. Soft fault occurring in sensor nodes can be identified using distributed approach. The soft faults are regarded as the one where sensor node is communicating byzantine readings. Such readings degrade the overall network performance. The Neyman-Pearson detection method is used to determine the faulty sensor node. Time and message complexities are calculated and analyzed by comparing it with existing techniques. The algorithm consists of four phases and in last phase based on Neyman-Pearson lemma; each sensor node decides apparent fault detection about neighbor nodes. Simulation in NS3 examines the performance of the proposed algorithm against three existing algorithms by evaluating different parameters. An increase in the total number of faulty sensors decreases detection accuracy. Implementation results depict progress in detection accuracy and false alarm rate as compared to existing work [8]. Fault detection and routing scheme are used to determine 5 types of hardware faults in sensor node. Whenever a node is stamped as faulty, it is no longer utilized in wireless sensor network. If a node is faulty due to some hardware faults, then it can still be utilized by determining its fault type. The proposed algorithm categorizes the faulty node to be reused as traffic node, normal node and end node depending upon the services it can cater. The simulation is carried out in ns2 to evaluate three performance metrics as time elapsed, energy loss rate and number of healthy nodes. Distributed method uses cellular automata wherein cluster head works with regard to local information. Cluster head makes a decision about its member nodes responsibilities. The paper highlights function fault. The paper also proposes the L- system based routing scheme for data routing using normal or traffic node. Faulty sensor nodes are reutilized to work according to their remaining hardware capabilities [9].

Faulty node detection algorithm, centralized in nature classifies the nodes relying on their sensing output and spatial distance from the event to detect the node with data fault. Real time pre-processing experiment on radio and acoustic signal implies that sensor readings help to find the relative distance between the node and event. The three stage algorithm outputs blacklist of nodes by analyzing inconsistencies between detected and estimated sequences. Two metrics, i.e. the false negative rate and false positive rate are used to estimate the performance of the proposed method using data from real world experiments. Extensive simulations are performed to test the algorithm on large scale deployment. The experimental results achieve reduced false negative rate and false positive rate for different network scenario [10].

A deep belief network (DNB) can be used to distinguish fault data from normal data. It proposes a maximum squared error technique to identify faulty sensor from data. The generalized likelihood ratio test (GLRT) is used for categorizing the type of fault. The number of faulty data recorded by the sensor is used for fault pattern classification. Thermocouple failure signals are studied and proposed method is evaluated on it. It is able to identify all fault types except stuck at fault. The nuclear power plant thermocouple sensor tests for multiple sensor faults to help in deciding maintenance or replacement of sensors. The different fault types of thermocouples like noise, gradual, open and short are discussed in detail and composite GLRT method helps to identify the exact fault [11]. A distributed approach using Bayesian probability to detect sensor nodes with data fault introduces border nodes to increase accuracy of faulty node detection in a densely deployed WSN [12]. It works to assess the fault probability of a sensor node with the help of neighbor nodes and then the probability is adjusted by border nodes which greatly reduce the misdiagnosis. It presents performance comparison with similar approach presented in DFD algorithm by[13]. The simulation is carried out in MATLAB with two metrics fault node detection accuracy and false alarm rate. The faulty temperature sensor node reading is kept very high as compared to good node. This method suits well for faulty sensors with outlier faults but it would be interesting to observe its performance accuracy for constant or low reading faults. Abnormal sensor events can be detected when the monitored process behavior pattern is known beforehand. The pre-processing stage models behavior of sensor in normal and dynamic operating condition. The factors affecting sensor data flow are analyzed. The substantial change in variation from sensor output is considered an abnormal behavior. The method is implemented on real life IoT platform with real sensors. The method fails to highlight situation where sensor readings cannot be modeled aforementioned [14]. Fault detection of sensors and fault tolerance of a network are studied together in union. Due to low cost of sensors, the authors propose the use of duplex sensor i.e. one active sensor and one inactive standby sensor. Reliability is achieved by introducing redundancy. A sensor node model which is non fault tolerant is used to propose a fault tolerant WSN cluster model. Two existing distributed faulty node detection methods are simulated in NS2 and fault tolerance is incorporated using Markov models. Experimental results indicate that the proposed fault tolerant model gives remarkable improvement for MTTF if fault detection algorithm gives better accuracy [15].

III. GAP ANALYSIS

Literature survey discusses about existing faulty node detection and fault tolerant techniques in wireless sensor network. A sensor fault may be a data fault and hardware fault. Binary sensor output is different from usual sensors. Data fault model applicable to binary sensors needs to be handled differently as there are only two possible outputs. The interpretation of output from binary sensors may lead to ambiguity. Spatial and temporal aspect of sensors may help to tackle this ambiguity. The existing literature lacks in highlighting the following aspects of binary sensors.

- Mapping of data faults occurring in binary sensors to that of conventional sensors.
- Binary sensor data fault needs to be studied in detail by analyzing the functioning of binary sensors.
- A data fault model applicable to binary sensors and investigating methods to identify data faults.

IV. OVERVIEW OF BINARY SENSORS

Binary wireless sensor network (BWSN) is a wireless sensor network which consists of binary sensor nodes. BWSN functioning is same as normal WSN. The binary sensor node is suitable due to its characteristics. Binary sensor is specified as a sensor which outputs a binary value. Binary sensors are the one whose result is a Boolean value.

A. *Binary Sensors*

When a wireless sensor network uses binary sensors it is named as a binary wireless sensor network. The sensor nodes, which follow the binary sensing model, are known as binary sensors. In the binary sensing model, a sensor node records its observations with just a single bit. Specific applications like event detection, monitoring of phenomenon are interested in knowing for e.g. whether a particular event has happened or not. The applications didn't need real values, but just Boolean answer. In such scenarios, binary sensors are relevant. Binary sensors have numerous benefits. As the sensors report a single bit outcome, it saves communication bandwidth. Signal processing in sensor becomes relatively becomes easy. The communication network has to convey just single bit that also when the phenomenon is evident else it doesn't send any bit. Hence the usage of binary sensors can greatly lessen the burden on the communication network, thereby increasing performance and efficiency.

B. *Binary Sensing Model*

Binary sensors outcome depends on the threshold of the phenomenon being observed. Sensors experiencing value less than the threshold remain silent. When the sensor node records observation above threshold, it reports single bit value '1' to the sink node.

Let us consider binary sensors whose output is a single bit value. The single bit value can be either '0' or '1'. So here binary sensors will take decision based on comparison of the observed data and threshold. So in BWSN, binary sensors will send '1' when the observed data exceeds certain threshold. The observed data of the i^{th} sensor where $i = 1..P$, at time t where $t = 1..Q$, is given by

$$S_i(t) = \begin{cases} 1 \text{ if } x(t) \geq T \\ 0 \text{ if } x(t) < T \end{cases} \quad (1)$$

Where x(t) is the observed data at i^{th} sensor and T holds a predefined threshold value. The sensor will send only one bit information. From equation (1), if the data measured at S_i exceeds the threshold value T then it will send a single bit value '1' to the sink node. If the data measured at S_i is below the threshold value T then it will remain silent. From the communication network perspective,

if $(S_i(t) = =1)$ then

$C(S_i - S_j)$ exist,

where $C(S_i - S_j)$ indicates routing a bit information from S_i to S_j to reach finally to sink node.

C. *Network Model*

Binary wireless sensor network consists of a set S of N static sensor nodes given as $S=\{S_1, S_2,..S_N\}$ randomly spread across a field and communications among any pair of sensor nodes is present. Each Sensor node S_i knows its position $L(x_i,y_j)$. The transmission range T_r of all sensors is assumed to be same. If the distance between two sensor nodes is less than T_r then the two sensor nodes are able to send data to each other. So neighboring nodes of sensor node are all nodes which are one hop distance away or in other words, for any two nodes S_i and S_j and Distance D between them is such that if $D(S_i, S_j) < T_r$ then S_i and S_j are neighbors.

All the sensor nodes in the binary sensor network are connected by a wireless interconnection network. Communication amongst sensor nodes such as sending and receiving the messages occur within a stipulated time.

D. *Binary Sensors Data Fault Model*

Binary sensors can exhibit only two values '1' or '0'. The classification of faults into constant and varying types goes well with binary sensors faults. Categorization of different faults associated with sensors are discussed[16].

Data fault in a sensor node is the incorrect data sent to the sink node. Data fault can be examined with respect to time and space domain. Sensors in a neighborhood of an event are expected to send consistent result. If the event occurs for certain duration then sensors in the vicinity of the event are supposed to show same result for the duration of the event.

The faults in binary sensors can be classified by understanding different sensor data faults in general. It is assumed that all fault free sensor nodes in sensor networks are giving same output at any given instant of time t. The faulty sensor nodes reports inaccurate data. The data of sensor node Si at time instant t denoted as $S_i(t)$ is generated from normal Gaussian distribution with mean A and variance σ^2 i.e. $S_i(t) \sim N(A,\sigma^2)$. The data model assumes that all fault free sensor nodes should have same mean A however the measured noise of different sensor node may be different. This type of assumption is usually observed in literature related to detection of faulty sensor nodes in WSN[17]. False positive and false negative behavior of sensors clearly indicates that they are giving exactly opposite results from what they are supposed to deliver.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

The faults occurring in binary sensors here might be temporary or permanent. Three types of data faults are identified for binary sensors as shown in fig 1.

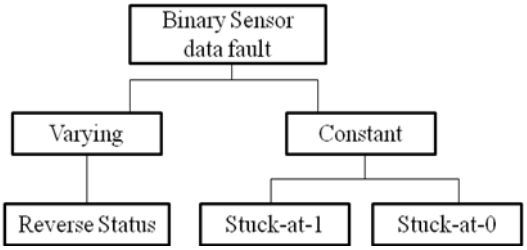

Figure 1 Data faults classification in binary sensors.

1) Reverse Status: Binary sensors may report the contradictory readings than the expected one. The nodes which are supposed to be alarmed remain unalarmed are called as false negatives. The nodes which are outside the event range are supposed to be unalarmed became alarmed are called as false positives.

2) Stuck-at faults: A sensor measurement may get fixed to a specific value for a time interval. In case of binary sensors there are two types of stuck-at fault possibilities. When the sensor node is not in event range and still it constantly reports the occurrence of an event that is a sequence of false positives, then it is stuck-at'1' fault. When the sensor node is in the event range and still it constantly does not report the occurrence of the event that is a series of false negatives then it is stuck-at'0' fault. Stuck-at faults may happen due to a variety reasons. These faults can be attributed to processing board's excessive heating, low battery level, detection threshold being wrongly programmed, power depletion etc[18].

Further reverse status and stuck-at faults of binary sensors can be analyzed with respect to faults occurring in conventional sensors. Conventional sensors usually exhibit following four types of data faults[19].

1. Outlier: An outlier is defined with respect to time and space domain. In the time domain, it is an isolated sample whereas in space domain it is remarkable change of data than expected Context information about event and sensors greatly helps in identification of this fault.

2. Spike: At least few sensor readings combinations will point this type of fault. The readings may not reveal the expected behavior of the phenomenon. The reading cannot always be interpreted as a fault, but certainly its ambiguity leads to suspicious marking followed by further investigation.

3. Stuck-at: The sensor readings are stuck to a specific value. This no variation in reading must be supported by the expected behavior of the phenomenon. The sensor might operate normally after the fault or it may not. The sensor value may be stuck to value of expected or unexpected range. Neighborhood relation can be utilized to determine whether the sensor is faulty or good if the value at which the sensor is stuck lies in the expected range. In cases where the stuck-at value is within the expected range, spatial correlation can be utilized to identify whether the stuck sensor is faulty or functioning appropriately.

4. Noise: Unexpectedly high degree of variation in sensor readings. The readings may or may not point towards the occurrence of expected behavior.

Table I Analysis of data faults in binary sensors with respect to faults in conventional sensors.

Conventional sensor fault	Binary sensor fault interpretation
Outlier	Random, reading 1 or silent from an sensor.
Spike	Two neighborhood sensors show different reading. One sensor sends a bit value 1 and other sensor remains silent. It is observed for a single instance at a time.
Stuck- at	Sensor reading might get stuck up to a particular value either1 or silent, for a certain time period or permanently.
Noise	The sensed reading is either very high or very low when compared to the proper working sensors readings. The sensor can send bit value 1 or remain silent.

V. PROPOSED ALGORITHM FOR BINARY DATA FAULT DETECTION (BDFD)

To evaluate how sensor neighborhood information can be utilized at the base station in order to enhance detection accuracy of faulty binary sensors, we first discuss the binary wireless sensor network scenario where this proposal can be applied. As discussed earlier, our work specifically targets data fault detection in binary sensors. In event detection applications, the network is formed from a large number of nodes to sense a phenomenon with constraint for computation power, memory and energy. The constraints can be handled effectively with the use of binary sensors.

A. *BDFD Algorithm*

Binary Wireless Sensor network for event detection application with data faults in some sensors is depicted in fig 2. The event occurred should be noticed by the sensors falling in the range denoted by dotted circle. All the sensors which are fault free and within the range should send bit value '1' to sink node.

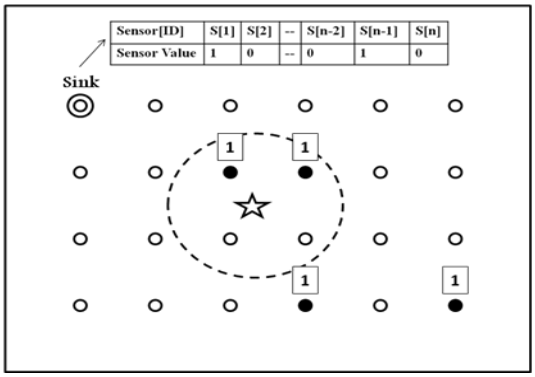

Figure 2 Binary wireless sensor networks with data faults in sensors. A sink node maintains a table about sensor neighbours and its output value.

☆Event occurrence, ○ Sensor, ( ) Event Range, ● Sensor detecting an event

A sink node maintains a table SNT where the value received from the sensor is stored for further processing. Initially it assigns a value '0' to all sensors. This table also helps to analyze the spatial relation amongst neighboring sensors. It also helps to determine the temporal relation amongst neighboring sensors by analyzing it over a period of time

Eventually, when an event occurs, sensors start responding by sending value '1'. It is assumed that if the sensor sends a bit that means it has detected the event otherwise it remains silent. In fig. 2, out of the four sensors in the dotted circle only two detect the event and send value '1' to the sink node. The remaining two nodes are silent as they are faulty. Two nodes outside the event range are also sending '1' to sink node which makes them faulty. Faulty nodes inside the circle are false negative instances as those are supposed to detect the event, whereas faulty nodes outside the circle are false positive instances which were supposed to remain silent. The nodes which detect the event correctly are healthy. False positive and false negative nodes are faulty.

Table II Notations used in the proposed BDFD algorithm

Symbol	Description
S	Set of sensor nodes, $S=\{S_1,S_2,..,S_N\}$
$N(S_i)$	Set of Neighbors of sensor node S_i
SNT	The sink node table containing information about sensors, their output and neighbors
R_i	Binary reading of sensor node S_i
C_i	Total number of Si's neighbor with reading '1'
$n(S_i)$	Total number of S_i's neighbor nodes, $n(S_i)= \|N(S_i)\|$
$F(S_i)$	Fitness value of Sensor, $F(S_i)=\{A,ST1,H\}$ where A: Ambiguous, ST1: Stuck-at '1', H: Healthy

Proposed algorithm counts the total number of sensor's neighbor whose binary decision is same as the sensor in question by exploiting spatial correlation. This helps to temporarily decide the health status of sensor. However when the sensor's binary decision is observed for a certain time period along with its neighbors binary decision, it will help to decide permanent health status of that sensor.

Algorithm: Binary Data Fault Detection

```
1   Each sensor node Si's reading is collected at
    sink node in SNT at every time cycle
2   Repeat following method every time cycle.
3   for each sensor node Si with Ri = =1 do
        Initailize Ci =0;
4       for each neighbor Sj ∈ N(Si) do
5         if Rj = = 1 then
6           Continue;
7       else
8           Increment Ci by 1;
9       end if
10    end for
11    if Ci >= (n(Si)/2) then
12        F(Si)= A;
13    else if Ci = = n(Si) then
14        F(Si)=ST1;
15    else
16        F(Si)=H;
17    end if
18  end for
```

When more than 50% of a sensor's neighbor are silent then the fitness value 'A' corresponds to ambiguity as the node might be faulty due to reverse status or stuck-at'0' fault. Basically in reverse status fault, a sensor might send exactly opposite value after certain time. Only time series analysis can throw a light on it. When all neighbors of a sensor are silent but the sensor itself is reading value '1' then it is a solo instance and it implies that the sensor is faulty due to stuck-at'1' fault.

This is centralized approach which tags nodes into faulty or healthy. The algorithm utilizes space and time domain both. To tag a node permanently as faulty, a further analysis of a sensor's neighbor response and its behavior over a period of time needs to be carried out. For example, analyzing the behavior for successive cycles, we can nail a node as faulty or healthy.

VI. Results and Discussion

In pursuance of evaluating the accuracy of the proposed binary data fault detection algorithm, a series of simulation were conducted using network simulator NS2. Simulation was carried out with 100 nodes deployed in a random manner.

Table II Simulation Parameters

Parameter	Value
Simulator	NS2
MAC	802.11
Simulation time	20s
Sensor Deployment area	1200x800 m^2
Number of nodes	100
Fault model	Normal random variable
Transmission range	40m

A simulation is run with different configuration which includes variation in number of faulty sensors like 10%, 20% and 30%.

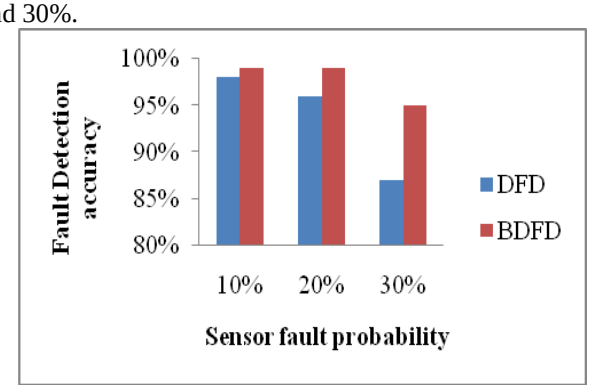

Figure 3. Fault detection accuracy for varying number of faults.

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication (BEIESP)

BDFD algorithm performance is compared with Fault Detection algorithm DFD proposed in [13]. DFD algorithm uses local neighborhood information for majority voting in order to establish truth about data measurements. In the first run, out of 100 nodes, 10% nodes were deployed faulty and the results are compared with and it is seen that accuracy of BDFD is improved by 1%. With 20% faulty nodes in the network, the accuracy of BDFD was improved by 3%. The accuracy recorded by BDFD in the presence of 30% faulty nodes was enhanced by 8% with respect to DFD. It is still about 95% when there are 30% sensors faulty. The main aim of the evaluation was to study the impact when number of the faulty sensors is increased with respect to existing and proposed algorithm. From fig. 3, it is observed that BDFD performs better even though the number of faults in the network is increased. The average number of neighbors was 5.

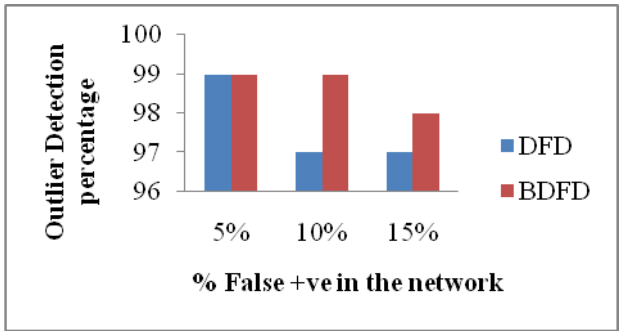

Figure 4. Outlier detection accuracy for varying number of fault positives.

BDFD algorithm is able to detect faulty nodes with isolated value '1' i.e. false positives or in other words an outlier instance as shown in fig 4. These outlier are instances of stuck-at '1' fault described earlier. Due to the random occurrence of faults, the detection accuracy varies. They will be tagged permanent stuck-at'1' type fault. Besides, if a node is not faulty then its neighbors who didn't report '1' will be observed using time series analysis to comment whether the event was not in their range or they were faulty as they remained silent. The ones who remained silent, though in the vicinity will be initially tagged temporary faulty or showing reverse status. After analysis, they may become permanent faulty marked as stuck-at '0' faults or may recover from the fault and become healthy. The accuracy will improve if the time series analysis is carried out for a long time period. But in real time applications, the fusion center has to provide quick response so a feasible time period should be considered depending on the applications. Evaluation metric is fault detection accuracy which is defined as the ratio of the number of faults detected to the total number of faults present in the network. The fault detection accuracy is more as compared to the existing algorithm as space and time domain are used to comment on the fault status. The spatial relation helps to identify temporary faulty sensors, but the temporal analysis helps to make the final decision on the health status of a sensor.

VII. CONCLUSION AND FUTURE WORK

Real time event localization application performance suffers due to faulty data by sensors. We proposed a binary data fault detection algorithm where sensor behavior over a time period is analyzed along with its neighboring sensor behavior to decide the sensor fitness. The proposed algorithm is evaluated by carrying out simulation. Our simulation results show that accuracy is not degraded even though the sensor fault probability is increased. The detection accuracy of proposed algorithm is increased by 8% with respect to existing algorithm when 30% nodes are faulty in the network. False positive instances, i.e. stuck at'1' fault identification is illustrious. Reverse status fault can be identified after time series analysis. Stuck-at'0' fault identification of nodes outside the vicinity of event is ambiguous as it is difficult to comment as it appears to be silent.

But as far as event localization application is considered, it is not going to affect the performance of locating an event. Applying the binary data fault detection algorithm in the event localization application is left as future work.

REFERENCES

1. Tolle, Gilman, et al.,"A macroscope in the redwoods," in *Proceedings of the 3rd international conference on Embedded networked sensor systems*. ACM, 2005, pp. 51-63.
2. Sharma, Abhishek B., Leana Golubchik, and Ramesh Govindan, "Sensor faults: Detection methods and prevalence in real-world datasets," *ACM Transactions on Sensor Networks (TOSN)*,2010, p 23.
3. Fang, Lei, and Simon Dobson, "In-network sensor data modelling methods for fault detection," in *International joint conference on ambient intelligence*. Springer, 2013 ,pp.176-189.
4. Miao, Xin, et al., "Agnostic diagnosis: Discovering silent failures in wireless sensor networks," *IEEE transactions on wireless communications*, 2013, pp. 6067-6075.
5. Rassam, Murad A., Anazida Zainal, and Mohd Aizaini Maarof, "An Efficient distributed anomaly detection model for wireless sensor networks," in *AASRI Procedia* 5, 2013, . 9-14.
6. Kamal, Abu Raihan M., Chris Bleakley, and Simon Dobson,"Packet-level attestation (PLA): A framework for in-network sensor data reliability," in *ACM Transactions on Sensor Networks (TOSN)* 9.2 ,2013, p. 19.
7. Bosman, Hedde HWJ, et al., "Spatial anomaly detection in sensor networks using neighborhood information," in *Information Fusion* 33, 2017, pp.41-56.
8. Panda, Meenakshi, and Pabitra Mohan Khilar, "Distributed Byzantine fault detection technique in wireless sensor networks based on hypothesis testing," in *Computers & Electrical Engineering* 48, 2015,pp. 270-285.
9. I. Banerjee, P. Chanak, H. Rahaman, and T. Samanta, "Effective fault detection and routing scheme for wireless sensor networks," Elsevier-Computers & Electrical Engineering, vol. 63, 2013,pp. 291-306.
10. Guo, Shuo, et al., "Detecting faulty nodes with data errors for wireless sensor networks," *ACM Transactions on Sensor Networks (TOSN)* 10.3, 2014, p. 40.
11. Mandal, Shyamapada, et al., "Nuclear Power Plant Thermocouple Sensor-Fault Detection and Classification Using Deep Learning and Generalized Likelihood Ratio Test," *IEEE Transactions on Nuclear Science* 64.6, 2017, pp. 1526-1534.
12. Yuan, Hao, Xiaoxia Zhao, and Liyang Yu,"A distributed Bayesian algorithm for data fault detection in wireless sensor networks," in *2015 International Conference on Information Networking (ICOIN)*. IEEE, 2015, pp.63-68.
13. Chen, Jinran, Shubha Kher, and Arun Somani, "Distributed fault detection of wireless sensor networks," in *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*. ACM, 2006, pp. 65-72.
14. Sándor, Hunor, Béla Genge, and Zoltán Szántó,"Sensor data validation and abnormal behavior detection in the Internet of Things," in *Networking in Education and Research (RoEduNet), 2017 16th RoEduNet Conference*. IEEE, 2017, pp.1-5.

15. Munir, Arslan, Joseph Antoon, and Ann Gordon-Ross, "Modeling and analysis of fault detection and fault tolerance in wireless sensor networks," *ACM Transactions on Embedded Computing Systems (TECS)* 14.1, 2015, p 3.
16. . Zug, Sebastian, André Dietrich, and Jörg Kaiser,"An architecture for a dependable distributed sensor system," *IEEE Transactions on Instrumentation and measurement* 60.2, 2011,pp. 408-419.
17. Krishnamachari, Bhaskar, and Sitharama Iyengar,"Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks," *IEEE Transactions on Computers* 53.3, 2004, pp. 241-250.
18. Laoudias, Christos, Michalis P. Michaelides, and Christos G. Panayiotou, "ftTRACK: fault-tolerant target tracking in binary sensor networks," *ACM Transactions on Sensor Networks (TOSN)* 10.4,2014, p. 64.
19. Ni, Kevin, et al., "Sensor network data fault types," *ACM Transactions on Sensor Networks (TOSN)* 5.3, 2009, p. 25.

AUTHORS PROFILE

Vaishali S. Deshmukh is the Assistant Professor in the Department of Computer Engineering at STES's Smt. Kashibai Navale College of Engineering, Pune, India.. She received her B.E. Degree in Computer Science and Engineering from Sant Gadge Baba Amravati University, Amravati, India. She received her M.E. Degree in Computer Engineering from Savitribai Phule Pune University, Pune, India. Currently she is pursuing PhD in Computer Engineering at Savitribai Phule Pune University, Pune, India. She has more than 16 years of teaching experience. She has published more than 20 research publications at national and international journals and conferences.

Arvind V. Deshpande is the Principal at STES's Smt. Kashibai Navale College of Engineering, Pune , India. He completed his Ph. D in Computer Science and Engineering. He has more than 28 years of teaching and research experience. He is member of Board of Studies in Computer Engineering, Savitribai Phule Pune University, Pune, India. He has also remained technical program committee member for International Conferences and Symposium. He has contributed in various research publications at national and international journals and conferences.

Parikshit N. Mahalle has obtained his B.E degree in Computer Science and Engineering from Sant Gadge Baba Amravati University, Amravati, India and M.E. degree in Computer Engineering from Savitribai Phule Pune University, Pune, India. He completed his Ph. D in Computer Science and Engineering with specialization in Wireless Communication from Aalborg University, Aalborg, Denmark. Currently he is pursuing his PostDoc at Aalborg University, Denmark. He has more than 20 years of teaching and research experience. He is a member of board of studies in computer engineering, Savitribai Phule Pune University (SPPU), Pune, India. He is IEEE member, ACM member, Life member CSI and Life member ISTE. He has published several peer reviewed journal papers and book chapters in leading research journals like Elsevier, Inderscience, Springer, IGI Global, ACM and IEEE conferences.