Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 5, May 2014, pg.297 – 303

RESEARCH ARTICLE

Energy Efficient Trust Dependable System for Wireless Sensor Networks

K.Anandaraj[1], N.Kumaratharan[2], D.Balasubramanian[3]

[1]PG Student, Department of IT, Sri Venkateswara College of Engineering, Anna University, Sriperumbudur, 602117, Tamil Nadu, India

[2]Professor, Department of IT, Sri Venkateswara College of Engineering, Anna University, Sriperumbudur, 602117, Tamil Nadu, India

[3]Professor, Department of IT, Sri Venkateswara College of Engineering, Anna University, Sriperumbudur, 602117, Tamil Nadu, India

[1] ana00734@gmail.com; [2] kumaratharan@rediffmail.com; [3] dbsmanian@svce.ac.in

Abstract— Accurately positioning nodes in wireless sensor networks is very important because the location of those devices and sensors is a critical input to many higher-level applications used for sensing. Faults occurring in the sensor nodes are commonly due to the sensor device and the environment which is harsh where the sensor nodes were deployed and used for data communication. To ensure the networks quality of service it is necessary for a WSN to be able to detect the faults and actions to be taken to avoid further degradation of the sensing service. The Extreme goal of this paper is to locate the faulty sensor nodes in the wireless sensor networks as well as to find trust for other nodes. We have propose an algorithm to deduct node fault using localized node fault detection and introducing Trust dependability to the non-faulty nodes for energy efficient data communication. The implementation complexity of this LF algorithm is less and the probability of correct diagnosis is high even in the presence of large fault sets.

Keywords— Localization; Feedback trust; Global Trust; Direct Trust; Indirect Trust

I. INTRODUCTION

Wireless sensors which are smaller in size consume less power and achieve high transmission rates. By adopting wireless sensor networks (WSNs), the cost of monitoring systems such as structural and environmental monitoring systems which are greatly reduced due to the eradication of expensive wiring. The small form factor of wireless sensors also introduces new applications that require mobility or portability, such as animal tracking and vehicle tracking. However, small form factors and low costs of sensors also render wireless sensors more predominant to faults and failures. The applications of Wireless Sensor Networks (WSNs) in which they are widely deployed in many areas such as military surveillance, medical, etc. The WSNs consist of small nodes which are limited in energy. Those nodes are randomly distributed in the area which is to be sensed and the communication of nodes in the sensor network is achieved through wireless communication of WSNs. Those Wireless Sensor Networks belongs to Low Range Wireless Personal Area Network group. A sensor failure is defined as when a sensor is in irrecoverable state of operation (e.g., not turning on or not responding).In contrast, a sensor fault is defined as when the sensor is outputting measurements but the measurements are intermittently or permanently corrupted by some faults. Various forms of sensor faults exist including excessive noise, drifts, random spikes and non-linearity in the sensor transduction mechanism. As wireless networks become increasingly prevalent, they make integrating new information into applications possible. Location

information is one such information that is very important for many applications.

Localization refers to determining the physical position is a template of wireless devices or a sensor node which can be either static or mobile. we first performed a detailed study on the robustness of a broad array of localization algorithms to attacks that corrupt signal strength readings. The characterization of the response of algorithms provides insights to be taken into consideration by system designers when choosing localization systems for deployment. From the detailed robustness study, we observed that attackers can cause large localization errors using simple techniques.

II. RELATED WORK

Node fault has been detected using the Pair wise linear relation but there are some errors like noise and small fluctuations that doesn't match with the filter designed for detecting spike fault. Also it is not determined that the fault that has been occurred is due to spike voltage or due to damaged system. In existing system ARX-based spike fault detection method which does not require the system-input information or the a prior establishment of reference sensors is used in proposed system for LTI physical systems. The method is based on pair-wise relationships of sensors, and these relationships are learnt online when the system is functioning normal. The algorithm gives good performance it only loses part of all its effectiveness under situations where a pair of sensors which are highly correlated.

Energy efficient lightweight dependable trust system (EETS) for WSNs, which employ clustering algorithms First uses a trust decision-making scheme is proposed according to the nodes identities and usage (roles) in the clustered WSNs, which will be suitable for the WSNs because it facilitates energy conservation. Due to cancelling feedback occurs between cluster members (CM) or between cluster heads (CH), the approach which can be significantly used to improve efficiency of the system whenever reducing the effect of fault nodes.

III. PROPOSED ALGORITHM

A. Spike fault detection in wireless sensor node

The error of a localization algorithm is defined as the distance that is calculated between the true location X and the estimated location X1. The Received Signal Strength (RSS) readings collected from these two wireless sensor nodes. We calculate the performance of our fault detection schemes using detection rates and receiver operating characteristics. Our experiment results provide strong evidence of effectiveness of fault detection algorithms with high fault detection rates and low false positive alarm rates. Correspondingly, we found that most of the fault detection schemes provide qualitatively similar performance.

ALGORITHM IMPLEMENTATION:-

- n: total number of sensors;
- p: probability of failure of a sensor;
- k: number of neighbour sensors;
- S: set of all the sensors;
- $N(S_i)$: set of the neighbors of S_i;
- x_i: measurement of S_i;
- dt_{ij}: measurement diff between S_i and S_j at time t,
- $dt_{ij} = xt_i - xt_j$;

Step 1: Each Sensor S_i tests every member of $S_j \in N(S_i)$ to generate test $C_{ij}\{0,1\}$
Using the following method:

1. Each Sensor S_i, set $C_{ij} = 0$ and compute d^t_{ij};
2. IF $\left|d^t_{ij}\right| > \theta 1$ THEN
3. Calculate $\Delta d^{\Delta ti}_{ij}$;

$IF\left|\Delta d^{\Delta ti}_{ij}\right| > \theta 2$ THEN $C_{ij} = 1$;

Step 2: S_i generates a tendency value T_i based upon its neighbouring sensors test value:

1. IF $\sum_{Sj \in N(Si)} C_{ij} < \lceil |N(Si)|/2 \rceil$, where $|N(Si)|$ is the number of the S_i's neighboring nodes THEN
2. T_i = LG;
3. ELSE T_i = LF;
4. Communicate T_i to neighbours;

Step 3: Compare the number of S_i's LG neighboring nodes with different test results to determine its status:

1. IF $\left(\sum_{Sj \in N(Si) and T_j} = LG^{(1-2Cij)} \right) \geq \lceil |N(Si)|/2 \rceil$ THEN
2. T_j = GD;
3. Communicate T_i to neighbours;

Step 4: For the remaining undetermined sensors do the following steps in parallel for Max d cycles:

1. For i = 1 to n
2. IF T_i = LG or T_i = LF THEN
3. IF T_j = GD $\forall\ S_j \in N(S_i)$, THEN
4. IF C_{ji} = 0 THEN
5. T_i = GD;
6. ELSE T_i = FT;
7. ELSE repeat
8. Communicate T_i to neighbours;

Step 5: If ambiguity occurs, then the sensor's own tendency value determine its status:

1. FOR each S_i, IF $T_j = T_k$ = GD $\forall\ S_j, S_k \in N(S_i)$, where $j \neq k$, and IF $C_{ji} \neq C_{ki}$ THEN
2. IF T_i = LG (or LF) THEN
3. T_i = GD(or FT)

Each node inside the interested area are tested by its neighbors. Test results are either 0 or 1 depending upon the measurement difference and threshold value. Tendency value Ti is finalized at the third iteration. the analysis results obtained by applying the Localized Fault Detection Algorithm. Four out of nine sensor nodes in the area are fault. The other five nodes are good and there is no ambiguity occurring in this example. Each node's neighbors with GD tendency value generate the same testing results when they determine the node's status.

B. Lightweight dependability-enhanced trust calculation

Concept of Trust Values:

In the setup phase, the networks are partitioned into clusters, each with a randomly selected cluster head from nodes in a created cluster. Each sensor node chooses a random number m lies between 0 or 1. If m<T(n) for node n, the node becomes a cluster head. This decision is based on the threshold T(n).

The trust relationship is generally expressed as a specific quantitative value. This value can be a real number between 0 and 1 or an integer between 0 and 100. In this work, we transform this value into an unsigned integer in the interval between 0 and 10. Although presenting the trust values as a real number or an integer may be insignificant in traditional networks, this issue is of critical importance for WSNs because of limited memory as well as transmission and reception power.

C. Intracluster Trust Evaluation

The trust evaluation approach at CMs is given by

$$\mathrm{Tx,y}(\Delta t) = \left\lceil \left(\frac{10 \times s_{x,y}(\Delta t)}{s_{x,y}(\Delta t) + u_{x,y}(\Delta t)} \right) \left(\frac{1}{\sqrt{u_{x,y}(\Delta t)}} \right) \right\rceil \quad (1)$$

i) CH-to-CM Feedback Trust Calculation:

Suppose in the existence of (n-1) CMs in a cluster. The cluster head will periodically broadcast the request packets within the cluster. In response, all CMs in the cluster will forward their trust values toward other CMs Then will maintain these trust values in a matrix, as shown below where is the direct trust of node on given equation. On the other hand, which means this value is the node's ratings towards itself. To reduce boasting of, this value will be discarded by CH during feedback trust aggregation.

ii) Dependability analysis against malicious attacks:

We analyze the dependability of the LDTS protocol against Faults on a trust management system. In clustered WSNs, the main attacks from malicious nodes primarily these include two kinds of patterns:

D. Garnished fault and Bad mouth attack

In such a fault situations, malicious nodes behave well and bad alternatively with the aim of remaining undetected while causing damage. For instance, garnished malicious nodes may suddenly admit to faults as they accumulate higher trust worth.

As long as obtained feedback is considered, malicious nodes can provide dishonest feedback to frame good parties and or boost the trust values of malicious nodes that admits to faults. This fault, referred to as the bad mouthing, is the most straightforward fault. After providing some evidence of the malicious nodes' objective, we can prove that our trust management system at both CM and CH levels is dependable against Faults from malicious nodes because this system can detect the malicious behavior and can prevent such nodes from fulfilling their own objectives.

$$\mathrm{R_{ch,y}}\ (\Delta t)\ \text{-}\left\lceil 10 \times E\left(\varphi(p|r,v)\right)\right\rceil \tag{2}$$

where the nearest integer denotes the probabilities of binary events

$$\mathrm{E}(\varphi(\mathrm{p}|\mathrm{r},\mathrm{v})) = (\mathrm{r}+1)/(\mathrm{r}+\mathrm{v}+2) \tag{3}$$

Analyzing (2) and (3) and (4), our feedback aggregation is found to be a lightweight method with some very simple mathematical formulas, which is suitable for resource-constrained nodes in a large-scale sensor network.

E. Trust model illustration

Each node evaluates trust worth of its neighbor nodes behavior by cross checking those neighbor nodes' redundant sensing data using its own result by overhearing. The Trust model evaluates the trust worth and each node maintains the details of neighbor's behavior with consistent count, inconsistent count, sensing success and sensing failure. Each node updates neighbor nodes' behavior table, when valid data, then increment the consistent count and if not valid, then increment the inconsistent count, since malicious node may inject the false data. Using sensing success and sensing failure we can find out selfishness and normality of each node, since malicious nodes may not participate in the detection process as well as regular activity to save power, which asks the nodes' behavior.

Trust model also includes the battery power, since less power device may not be used in detection process and selfishness behavior related the power. From these details we quantify the nodes' behavior with consistent factor, Sensing Factor and battery power and also to compute the trust factor and with following trust quantification process and computation process.

IV. SIMULATION RESULTS

In this section, they evaluate the performance of our proposed algorithm through the simulations. In this results are compared our proposed Localization algorithm with ARX Based algorithm based on four performance metrics: Packet Delivery Ratio, Throughput, Loss and False alarm rate. The reference network of our simulations consists of 100 nodes distributed randomly in an area of 50m x 50m. The simulation results and comparison of the proposed system were executed and analyzed using Network Simulator (ns-2).

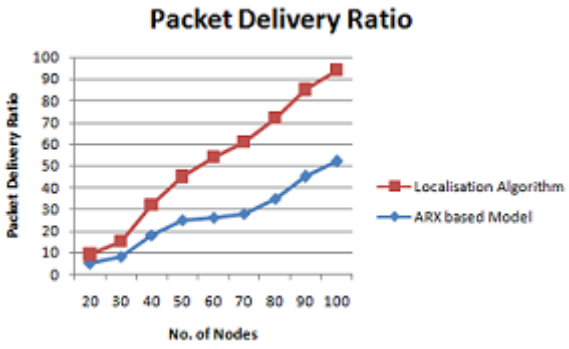

Figure 1: Packet Delivery Ratio

Figure 1 shows the Packet Delivery Ratio performance comparison between Localization algorithm and ARX Based algorithm WSNs. Compare to the exiting the proposed algorithm has improved Packet Delivery Ratio.

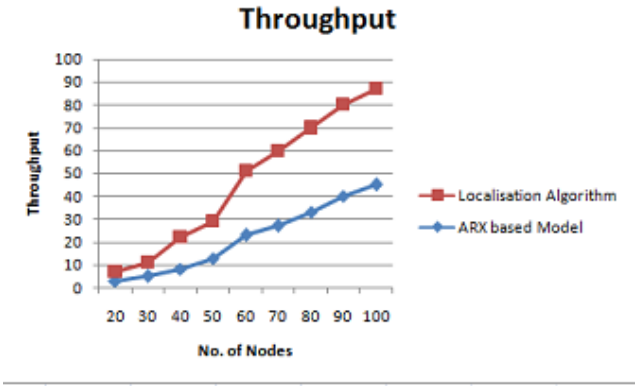

Figure 2: Throughput

Figure 2 shows the number of nodes are increased, corresponding Throughput is also increased. Compare the existing and proposed algorithm; the proposed algorithm has improved Throughput.

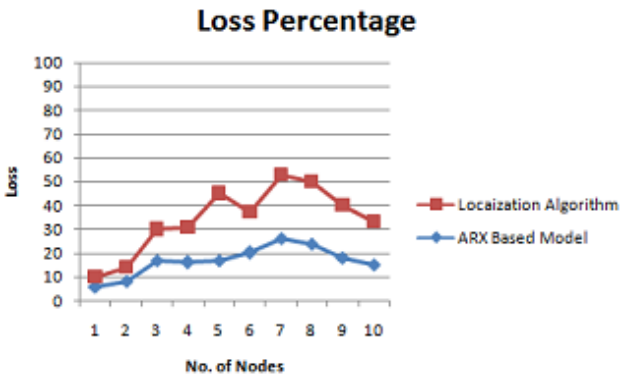

Figure 3: Loss Percentage

Figure 3 shows the proposed Localization algorithm is having decreased loss compared to the exiting ARX based algorithm. The number of nodes is increased, corresponding the loss is decreased. The performance comparison between Localization algorithm and ARX Based algorithm in WSNs. The number of nodes

increased, the **loss is decreased**. The proposed algorithm is reduced loss compared to the exiting algorithm**.**

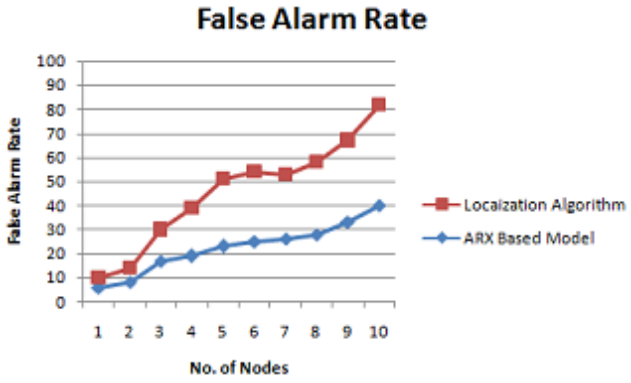

Figure 5: False Alarm Rate

Figure 4 shows, False alarm rate is increased, but the lifetime is decreased. The proposed algorithm is improved network lifetime compre than exiting algorithm.

V. CONCLUSION

In this paper, we use localized fault detection algorithm in wireless sensor networks and we are establishing trust relation between nodes on the basis of their prior interactions. This is efficient in establishing trust relations since it only counts on the direct interactions; however, it is lacking supervisors by other nodes. The mode with an addition of recommendation input part makes the supervisor by other nodes available to build trust in a more reliable way but less efficient (requiring extra local space for storing the recommendations) compared to the Localized algorithm. Our simulations result show that the Localized fault detection algorithm performs best in term of accuracy and Even though signatures bring additional costs, the proposed schemes are still affordable for WSNs after evaluation. Considering a large WSN, we also performed simulations on the proposed schemes.

Fault nodes are detected and further requirements and improvements could easily be done since these coding is mainly structured modular in nature. Improvements can be added by adding new modules of assigning the trust value calculations for the sensor nodes.

REFERENCES

[1] C. Lo, J. Lynch, and M. Liu(2011), "Reference-free detection of spike faults in wireless sensor networks," in Proc. 4th International Symposium Resilient Control System., pp. 148–153.

[2] V. Ricquebourg, D. Menga, M. Delafosse, B. Marhic, L. Delahoche, and A. Jolly-Desodt(1991), "Sensor failure detection within the tbm framework: A markov chain approach," in Proc. Information Process Management., p. 323.

[3] Sung-Jib Yim and Yoon-HwaChoi(2010), "An Adaptive Fault-Tolerant Event Detection Scheme for W ireless Sensor Networks"., Article sensors ISSN 2332-2347.

[4] J. Polastre, R. Szewczyk, A. Mainwaring, D. Culler, and J. Anderson(2004),"Analysis of wireless sensor networks for habitat monitoring," in Wireless Sensor Networks, USA: Springer-Verlag, pp. 399–423.

[5] Bhaskar Krishnamachari, Sitharama Iyengar(2004) "Distributed Bayesian Algorithms forFault-Tolerant Event Region Detection in Wireless Sensor Networks" IEEE Transactions on Computers, vol. 53, no. 3.

[6] J. Lynch, A. Sundararajan, K. Law, A. Kiremidjian, and E. Carryer(2004), "Embedding damage detection algorithms in a wireless sensing unit for operational power efficiency," Smart Mater. Structure, vol. 13, no. 4, p. 800.

[7] X. Dai, Z. Gao, T. Breikin, and H. Wang(2009), "Zero assignment for robust H2/H∞ fault detection filter design," IEEE Transaction. Signal Process., vol. 57, no. 4, pp. 1363–1372.

[8] R. A. Shaikh, H. Jameel, B. J. d'Auriol, H. Lee, and S. Lee(2009), "Group-based trust management scheme for clustered wireless sensor networks," IEEE Transaction Parallel Distributed. System. ,vol. 20, no. 11, pp. 1698–1712.

[9] L. Lennart (1999), "System identification: Theory for the user," in PTR Prentice Hall, NJ, USA: Upper Saddle River.

[10] F. Bao, I. Chen, M. Chang, and J. Cho(2012), "Hierarchical trust management for wireless sensor networks and its applications for trust-based routing and intrusion detection," IEEE Transaction Network Service Management., vol. 9, no. 2, pp. 169–183.

[11] T. Kobayashi and D. Simon(2003), "Application of a bank of kalman filters for aircraft engine fault diagnostics," DTIC, Fort Belvoir, VA, Tech. Rep.

[12] E. Aivaloglou and S. Gritzalis(2010), "Hybrid trust and reputation management for sensor networks," Wireless Networks., vol. 16, no. 5, pp.1493–1510.

[13] W. B. Heinzelman, A. P. Chandrakasan, and H. Balakrishnan(2002), "An application-specific protocol architecture for wireless micro sensor networks,"IEEE Transaction Wireless Communication., vol. 1, no. 4, pp. 660–670.

