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. 4, April 2014, pg.904 – 911

RESEARCH ARTICLE

DIAGNOSING SENSOR NODES AND DETECTING WORMHOLE ATTACKS IN WIRELESS SENSOR NETWORKS

R. Dhivya Subathra[1], M. Suguna[2], D. Sharmila[3]

[1]PG Student, SNS college of Technology, Coimbatore-641 035
[1] dhivyasubi@gmail.com

[2]Associate Professor, SNS college of Technology, Coimbatore-641 035
[2] suguna.marappan@gmail.com

[3]Professor, Department of EIE, Bannari Amman Institute of Technology

Abstract—*In Wireless Sensor Network, the multi-hop transmissions are used for data collection as well as to deliver a data packet by sequence of nodes. While transmitting the packets over a network, the faults occurring are common. In order to avoid faults and to ensure the network Quality of Service the WSN need to take actions for degradation of services. In existing system, the generic link model only considers the forwarding quality of a node using the metrics like packet delay, Packet Delivery Ratio, number of packets dropped but doesn't focus on the fault detection. The proposed system implements Distributed Localized Fault Sensor technique which helps to diagnose the sensor node during fault detection in a deployed area of sensor network. The diagnosis will complete if all the sensor nodes are identified as good or faulty in a predefined time. Thus the Localized Faulty Sensor Detection overcomes the problem of identification of faulty nodes in a sensor network and has considerable accuracy rate. As a result, the proposed system has a high fault detection accuracy and low false alarm rate. Individual sensor nodes are subject to be compromised in a security because they may be deployed in hostile environments and each sensor node communicates in a wireless medium. An adversary can produce a wormhole by directly linking two compromised nodes or using out-of-band channels to violate the security of a network. The proposed method uses ACK messages for detecting wormholes and is based on a Lightweight Countermeasure for Wormhole Attacks (LITEWORP) scheme. As a result the proposed method reduces energy consumption as well as provides greater network security.*

Keywords— ***Wireless sensor networks, QoF, Fault tolerance, Distributed algorithm, wormhole attack, compromised node detection***

1. INTRODUCTION

A wireless sensor network (WSN) is typically designed to span in a large field for data collection. Data delivery is normally attained with multi-hop transmission through a sequence of nodes. Most of the multi-hop routing protocols have been implemented in sensor networks for data

gathering and they usually accomplished with special path estimation metrics to choose "good" paths for data packets delivery. The tremendous advances in wireless communication and electronics have allowed the development of low cost and power, as well as the multifunctional wireless sensor nodes which consist of sensing, processing of data, and communication components. These tiny sensor nodes can easily be deployed into a designated area to form a wireless network and perform specific functions. With recent intensive research in this area, wireless sensor networks have been applied in various areas, such as environment and habitat monitoring, condition-based equipment maintenance, disaster management, and emergency response. Due to the low cost and the deployment of a large number of sensor nodes in an uncontrolled or even harsh or hostile environment, it is not uncommon for the sensor nodes to become faulty and unreliable. The networks must exclude the faulty sensors to ensure the network quality of service. To identify the faulty sensor nodes is not trivial at all because of the existing challenges. Sensor nodes are energized by rechargeable batteries, which are considered as limited resources. It is very expensive for the base station to collect information from the entire sensor and identify faulty sensors in a deployed area of a centralized way. Variety of applications must need the fault detection to be conducted in a real-time mode with low latency or high throughput. Therefore, a localized and distributed generic algorithm for each node is highly preferred in wireless sensor networks.

Fault-tolerance is the property that enables a system to continue operating properly in the event of the failure in some of its components. If its operating quality decreases at all, the decrease is proportional to the severity of the failure, as compared to a natively-designed system in which even a small failure can cause total breakdown. Fault-tolerance is particularly sought-after in high availability or life critical system. A fault-tolerant design enables a system to continue its intended operation, possibly at a reduced level, rather than failing completely, when some part of the system fails. The term is most commonly used to describe computer system designed to continue more or less fully operational with, perhaps, a reduction in throughput or an increase in response time in the event of some partial failure.

Network yield is mainly used to measure the quality of data gathering of the network. It measures the quantity of data received at the sink with respect to the total data generated by all the nodes over the network. The network yield can be calculated by

$$\text{Yield} = \frac{\text{Number of data pkts received at the sink}}{\text{Number of data pkts sent by all nodes}}$$

The network yield gives us the good throughput of the network, replicating both reliability of data forwarding and the network throughput. The packet loss is mainly due to two reasons. The first reason is transmission timeout on the links (exceeding the retransmission threshold); and the second reason is local packet drops within the node which are mainly due to receive/transmit queue overflow memory corruption, routing loops, packet duplication, and program bugs (e.g., race conditions) and etc. It will take a closer look at the causes of packet loss at individual sensor nodes.

2. RELATED WORK

Comprehensive and accurate measurement of path quality is an essential and crucial factor in identifying an effective routing mechanism for multihop wireless sensor networks. The QoF model

overcomes the limitation by simultaneously considering the quality of forwarding among nodes and link quality based on a generic link model. As analysed the experiments shows that the routing decisions yielded with QoF achieves less traffic cost as well as more end-to-end packet delivery ratio and minimizes the transmission cost also increases the data yield of the packet sent through the network.

Collaborative target detection is efficient in terms of communication cost of the nodes, accuracy, and number of tolerable Faulty sensors in the network. Two algorithms are used namely, value fusion and decision fusion. When comparing the performance and communication overhead, decision fusion is identified as better than value fusion as the ratio of faulty sensors to the fault free sensor increases. When the value fusion-based algorithm is found to perform better than decision fusion-based algorithms in the absence of faults. However value fusion-based and decision fusion-based algorithms performance become comparable as faults are injected in the system and decision fusion-based algorithms are preferred for lower communication overhead [1].

The distributed fault-tolerant detection in wireless sensor networks is mainly focused on two problems: 1) how to address both the noise-related measurement error and sensor fault simultaneously in fault-tolerant detection and 2) how to choose a proper neighborhood size n for a sensor node in fault correction such that the energy could be conserved. A fault-tolerant detection scheme that explicitly introduces the sensor fault probability into the optimal event detection process. The mathematical result shows that the optimal detection error decreases exponentially with the increase of the neighborhood size. Experiments approach in simulated sensor networks demonstrate that the proposed algorithm is able to achieve better detection and better balance between detection accuracy and energy usage [6].

A decentralized fault diagnosis system distinguishes between multiple root causes of degraded performance and provides efficient feed-back into the network to troubleshoot the fault. In particular, recent work has observed that one of the first order problems experienced in deployed WSNs is reduced data throughput. The root causes of the reduced sensor data throughput have been attributed in large part to either by hidden terminal conflicts, congestion, or wireless coverage/connectivity that exhibits irregular, asymmetric, and time varying behaviour. A decentralized fault diagnosis system is used for diagnosing faults in a sensor network and a new algorithm for effectively differentiating root causes of commonly experienced reduced data throughput [8].

Wormhole attacks are a powerful attack that can be conducted without need of cryptographic mechanisms. An attacker who conducts a successful wormhole attack is in a position to disrupt routing, deny service to large segments of a network, and use selective forwarding to tamper with network applications. Directional antennas offer a promising approach to preventing wormhole attacks. They are less expensive than many mechanisms proposed for localization, and offer other advantages in addition to security including more efficient use of energy and better spatial use of bandwidth. The protocols we propose reduce the threat of wormhole attacks with minimal loss of network connectivity. Given the lack of availability of other suitable defences and the potential damage a successful wormhole attack can inflict, this trade-off is desirable for many applications.[10]

In wireless sensor networks, the node communicates each other for exposing the information to provide the security over the attacks. A precise demoralizing attack is known as the wormhole attack, where a node which is considered as malicious registers the control as well as the data traffic at one site and tunnels it to a colluding node, which restate the information locally. This lead to adverse effect in route establishment by preventing nodes from discovering routes that are more than two hops away. A lightweight countermeasure for the wormhole attack (LITEWORP), which does not need any of the specified hardware. LITEWORP is mainly suitable for the purpose of resource-constrained multihop wireless networks, such as sensor networks. A detailed description of LITEWORP for networks, and discuss extensions to mobile networks. The solution allows wormhole detection along with isolation of the nodes which are called as malicious.[11]

3. NETWORK MODEL AN FAULT MODEL

The sensors are randomly deployed in the interested area and all sensors have a common transmission range. The area is assumed to be entirely covered by the sensors. The dark circles represent faulty sensors and the light grey circles are good sensors. There could be a failure occurring in a certain area. All sensors in the area go out of service. Since the nodes are depending on majority voting, it can be assumed that each sensor has at least 3 neighboring nodes. Because a large amount of sensors are cast into the interested area to form a wireless network on a deployed area, situation can be easily found out. Each sensor node is able to locate the neighbors within its transmission range through a broadcast/acknowledge protocol.

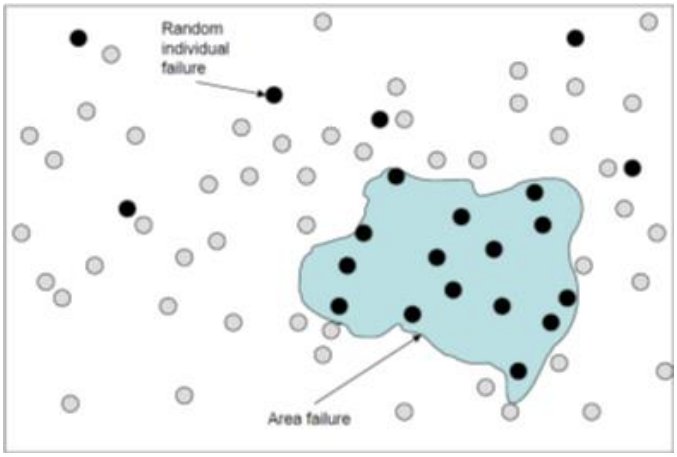

Figure 1: Sensor nodes randomly deployed over an area

4. LOCALIZED FAULTY SENSOR DETECTION

Definitions for the variables are mentioned and then, we present the localized fault detection algorithm.

4.1 Definitions

The list of notations used in our algorithm and analysis below,
- n: total number of sensors;
- p: probability of failure of a sensor;
- k: number of neighbor sensors;

- S: set of all the sensors;
- $N(S_i)$: set of the neighbors of S_i;
- x_i: measurement of S_i;
- d^t_{ij} : measurement difference between Si and Sj at time t, $d^t_{ij} = x^t_i - x^t_j$;
- $\Delta d_{ij}^{\Delta tl} = tl+1 - tl$;
- $\Delta d^{\Delta tl}_{ij}$: measurement difference between Si and Sj from time tl to tl+1, $\Delta d^{\Delta tl}_{ij} = d^{tl+1}_{ij} - d^{tl}_{ij} = (x^{tl+1}_i - x^{tl+1}_j) - (x^{tl}_i - x^{tl}_j)$;
- c_{ij} : test between Si and Sj , $c_{ij} \epsilon \{0, 1\}$, $c_{ij} = c_{ji}$;
- θ1 and θ2: two predifined threshold values;
- T_i: tendency value of a sensor, Ti ϵ {LG, LT,GD,FT};
- Maxd: an estimate of propagation distance from a set of identified good sensors in the first round of the algorithm iterations. The worst case is n, the best case is log n, and it take a reasonable √n.

Sensors are considered as neighboring sensors if they are within the transmission range of each other. Each node regularly sends its measured value to all its neighbors. Sensors are interested in the history data if more than half of the sensor's neighbors have a significantly different value from it. IThe nodes can use this $\Delta d^{\Delta tl}_{ij}$ to find if the current measurement is different from previous measurement. If the measurements change over the time absolutely, it is more likely the sensor is said to be faulty. A test result c_{ij} is generated by sensor Si based on its neighbour Sj 's measurements using two variables, d_{ij} and Δd_{ij} , and two predefined threshold value θ1 and θ2. If a sensor is faulty, it can generate arbitrary measurements. If c_{ij} is 0, most likely either both Si and Sj are good or both are faulty. Otherwise, if c_{ij} is 1, Si and Sj are most likely in different status. Sensors can be either LG or LF determined by using test value from its neighboring sensors. Each sensor sends its tendency value to all its nodes which are neighbor. The number of the LG sensors with coincident test results determines whether the sensors are GD or P FT. That is N(Si) and Tj = LG, If a GD sensor is identified in the network, its test result can be applied to diagnose neighboring sensors' status. The information can be propagated through the entire network to diagnose all other sensors whether it is good or faulty. he diagnosis is valid only if the diagnosis is stable with the test results, t. If there's no sensor being diagnosed, all the neighboring nodes are either didn't diagnosed or the nodes are diagnosed as faulty.

4.2 Algorithm

The localized faulty sensor detection algorithm is summarized in the following:
Algorithm (Localized Fault Detection):
Step 1: Each sensor Si tests every member of Sj ϵ N(Si) to generate test cij{0, 1} using the following method:
1: Each sensor Si, set cij = 0 and compute dt_{ij} ;
2: IF $|dt_{ij}| > \theta 1$ THEN
3: Calculate $\_d^{\Delta tl}_{ij}$;
4: IF $|\Delta d^{\Delta tl}_{ij}| > \theta 2$ THEN cij = 1;

Step 2: Si generates a tendency value Ti based upon it neighboring sensors' test value:
1: IF $\sum_{Sj \epsilon N(Si)} c_{ij} < d|N(Si)|/2\rceil$, where |N(Si)| is the number of the Si's neighboring nodes THEN
2: Ti = LG;
3: ELSE Ti = LF;

4: Communicate Ti to neighbors;

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

1: IF ($\sum_{Sj \epsilon N(Si)}$ and Tj=LG(1−2cij) _ d|N(Si)|/2⌉ THEN
2: Tj = GD;
3: Communicate Ti to neighbors;

Step 4: For the remaining undetermined sensors, do the following steps in parallel for Maxd cycles:

1: FOR i = 1 to n
2: IF Ti = LG or Ti = LF THEN
3: IF Tj = GD Sj ϵ N(Si), THEN
4: IF cji = 0 THEN
5: Ti = GD;
6: ELSE Ti = FT;
7: ELSE repeat
8: Communicate Ti to neighbors;

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

1: FOR each Si, IF Tj = Tk = GD
Sj , S_k ϵ N(Si), where j ≠ k,
and IF cji ≠cki THEN
2: IF Ti = LG (or LF) THEN
3: Ti = GD (or FT)

Test results c depends on the threshold value of θ, which can be explained according to many applications at the deployment time. In step 1, it can also set two θ1 and θ2 values to be different. Step 5 is a validation check to make sure the diagnosis is consistent throughout the entire network.

5. LIGHTWEIGHT COUNTERMEASURE FOR WORMHOLE ATTACKS (LITEWORP)

LITEWORP is a countermeasure for wormhole attacks that does not require specialized hardware such as GPS. In the LITEWORP scheme, neighboring nodes common between two nodes are chosen as their guard nodes, which monitor the incoming and outgoing traffic of their neighbors. LITEWORP is operated in two phases as follows:

5.1 WORMHOLE DETECTION

Guard nodes monitor every incoming and outgoing data packet of its neighbor nodes. When a node sends a data packet to a receiving node, the guard nodes save the packet information in a watch buffer. The information includes the packet's identification and type, source, destination, and an immediate sender and receiver. The guard nodes expect that the receiving node will forward the packet toward the base station unless the receiving node is itself the base station. Each entry in the watch buffer has a time threshold; the receiving node must send the packet onwards before the time threshold expires. A malicious activity counter is maintained by each guard node. The malicious activity counter is incremented for each neighbor node malicious event that is detected by the guard node.

5.2 ISOLATION

When the malicious activity counter of node A crosses a threshold, the guard node revokes node A from its neighbor list, then sends alert messages to each neighbor node of node A indicating that node A is a suspected malicious node. When a neighbor node X of node A receives the alert, it stores the identity of the guard node in an alert buffer associated with A. When the number of alert messages regarding node A is over the threshold for node X, node X removes node A from its neighbor list. After isolation, node X does not receive or send any packet to a revoked node. Nodes that transmit reports wait for ACK messages after sending reports, but if the ACK messages do not arrive until after time t, the next node is regarded as a wormhole. Therefore the sending node eliminates the next node in the routing path, and then retransmits the reports to another node. The CoS node sends a report to the BS, and each intermediate node sends an ACK message to detect wormholes. All nodes that transmit reports must wait for ACK messages. It means all nodes that receive reports have to reply with ACK messages. The ACK messages are used to detect wormhole links. When node A sends a report to node B and node B sends it on to node C, node C replies with an ACK message to a neighbor node common to nodes B and C. Furthermore, nodes receiving ACK messages (node X) also send ACK messages to neighbor nodes common to node B and itself.

This operation is repeated until the ACK message is delivered to node A. Since node A sends the reports, it waits for an ACK message, which it cannot receive. The node B sends an ACK message to node A, but the ACK message has a maximum hop limit called Time-to-Live (TTL). If no limit was set, the ACK messages would float throughout the network, wasting limited node energy. It shows that node B sends an ACK message to node A with a limited TTL value, but the ACK message cannot be delivered to node A. If the TTL value is too large, it may be delivered to node A even when reports are transmitted via a wormhole. If the TTL value is too small, it may not be delivered to node A even when reports are not transmitted via wormhole. Therefore the TTL value must be carefully determined based on network statements.

6. CONCLUSION

The proposed system uses Localized Faulty Sensor algorithm which diagnosis the sensor node in high accuracy during the fault detection. The faulty nodes can be detected by means of one good sensor node within its transmission range. By varying the node mobility and the packet rates the throughput, routing control overhead, packet delivery ratio and end to end delay are measured and graphs are plotted in the quality of forwarding.

As a result a distributed localized faulty sensor (DLFS) detection algorithm where each sensor identifies its own status to be either ”good” or ”faulty” and the claim is then supported or reverted by its neighbours as they also evaluate the node behavior. The simulation results show that the FSDA is diagnosed correctly even 25% nodes are faulty. The FAR is very accurate when the sensor fault probability is low. By using Lightweight Countermeasure for Wormhole Attacks (LITEWORP) scheme the wormhole attacks has been detected accurately. As a result the scheme leads to proper routing for data transmission and decreases energy consumption.

REFERENCES

[1] Thomas Clouqueur, Kewal K.Saluja, and Parameswaran Ramanathan (2004), “Fault Tolerance in Collaborative Sensor Networks for Target Detection”, IEEE transactions on computing, Vol: 53, No: 3.
[2] Min Ding, Dechang Chen Kai Xing and Xiuzhen Cheng (2005), “Localized Fault-Tolerant Event Boundary Detection in Sensor Networks”, INFOCOM, Vol: 2

[3] Koushanfar, F.Potkonjak and M.Sangiovanni-Vincentelli (2003), "On-line fault detection of sensor measurements", IEEE Proceedings, Vol: 2.
[4] Krishnamachari. B and Iyengar.S (2004), "Distributed Bayesian algorithms for fault-tolerant event region detection in wireless sensor networks", IEEE Transactions on Computers, Vol: 53.
[5] Mahmood A and McCluskey E.J (1998), "Concurrent error detection using watchdog processors-a survey", IEEE Transactions on Computers, Vol: 37, No: 2.
[6] Luo X, Ming Dong and Huang Y (2006), "On distributed fault-tolerant detection in wireless sensor networks", IEEE Transactions on the Computer Networks, Vol: 55, No: 1.
[7] Kui Ren, Kai Zeng and Wenjing Lou (2008), "Secure and Fault-Tolerant Event Boundary Detection in Wireless Sensor Networks", IEEE Transactions on Wireless Communications, Vol: 7, No: 1.
[8] Sheth A, Hartung C and Han R (2005), "A Decentralized Fault Diagnosis System for Wireless Sensor Networks", IEEE International Conference on Mobile Adhoc and Sensor Systems Conference.
[9] Shan Lin, Gang Zhou and Yafeng Wu (2009) "Towards Stable Network Performance in Wireless Sensor Networks", Real-Time Systems Symposium.
[10] Lingxuan Hu,David Evans (2004), "Using Directional Antennas to Prevent Wormhole Attacks", Network and Distributed System Security Symposium.
[11] Issa Khalil, Saurabh Bagchi, Ness B. Shroff (2000) "LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks", Conference on Electrical & Computer Engineering.
[12] Levente Butty´n, L´szl´ D´ra, and Istv´n Vajda (2008), "Statistical Wormhole Detection in Sensor Networks",Laboratory of Cryptography and System Security (CrySyS) conference.
[13] Tsang-Yi, Wang Han, Y.S. Varshney and P.K. Po-Ning Chen (2005), "Distributed fault tolerant classification in wireless sensor networks", IEEE Journal on Selected Areas in Communications, Vol: 23, No: 4.
[14] Chun Lo, Ann Arbor, Mingyan Liu , Lynch and J.P. Gilbert (2013), "Efficient Sensor Fault Detection Using Combinatorial Group Testing", IEEE International Conference on Distributed Computing in Sensor Systems (DCOSS).

