International Journal of Advanced Research in

Computer Science Engineering and Information Technology

Volume: 3 Issue: 1 26-Jun-2014,ISSN_NO: 2321-3337

SURVEY ON FAULT LOCALIZATION TECHNIQUES IN WIRELESS NETWORKS

B.Usha Ranjini,Dr.T.Ravichandran

Asst. Professor, MCA, V.S.B.Engineering College, India.
Principal, Computer Science, Hindustan Institute of Technology, India

.

ABSTRACT— *Wireless sensor networks (WNS) are widely used distributed networks to contact with the real world in various applications such as Environmental Monitoring, Vehicle Tracking and Mapping, and Emergency Response. The main problem in such application is to identify the node position; challenges in wireless sensor network are to have communication between the nodes under limited resources and processing noisy data without any reduction. So the methods for localization using range based techniques are calculated. These techniques will limit the fixed and mobile nodes for effective communication. Similarity Hashing Function and an Identity based Combined Signature allows nodes to check incoming encoded packets, and introduces an efficient mechanism to reduce the computation overhead and protect from effluence attack. Performance evaluation of various localization techniques are analyzed in terms of fault detection efficiency, communication overhead, average error rate, time consumption and packet loss rate.*

Keywords — Localization, Anomalies, Protocols, Analysis, Parameters

1, INTRODUCTION

A wireless sensor network is distribution of nodes which are constrained of resources and with little user work. The motion patterns of the node within the network are very important because the nodes have to move freely but within the limited access. There are many tasks to be done in order to maintain the network efficiency as there will be many faults in the movement of nodes, communication between the nodes, check the incoming packets and also to protect the network from any malicious attacks. To solve the faults in the network between the nodes a fault localization technique is needed to detect the fault and also recover the network from the fault. There are two phases in this technique

- Fault diagnosis
- Fault Recovery

Localization is used to detect and record the events happening in the network and also route the packet. Manual configuration is difficult for large scale networks when the nodes of the network are in motion. The self localization problems for the mobile nodes are solved by using multi model auxiliary particle filters [1], but when fixed and mobile nodes try to communicate the problem will arise. Secure Wireless Network Connectivity with Multi-Antenna Transmission [4] improves secure connectivity by forming a directional antenna but not extended to the local to global connectivity. To solve these

problems Anchor Free Movable Topographical Scattered Localization (AF-MTSL) technique localizes both fixed and mobile nodes for effective communicate with each other. AF-MTSL technique in wireless networks supervise a moving space for every node, and then uses measures to sense any movement of each node.

Integrated detection and diagnosis framework identify anomalies and find the most probable root cause [2]. Integrated detection and diagnosis framework faces the most complex fault cases on different characteristics impact. To overcome these issues, focus is made on developing Self Fault Diagnosis model (SFD) for fault detection and diagnosis. Other problems are solved by using Similarity Hashing Function (SHF) and individuality based aggregate signature which allows sensor nodes to check packets on the wing before they accept incoming encoded packets.SHF introduces an efficient mechanism to reduce the computation overhead at each node and to eliminate bad packets quickly.

This paper is organized as follows: Section II discusses the Fault Localization Techniques. Section III shows the analysis of recent techniques in Fault Localization through similarity hashing. Section IV describes the literature review in tabulation form by comparing the complete Fault Localization Techniques. Section V terminates the paper, solution areas of future research to expand their real world applications. Section VI discusses the future direction of these systems.

2, Fault Localization Techniques in WSN

Identifying location of the nodes is very important in WSN as without the location information we cannot find the fault at which place it occurred and we don't know where the data is coming from. To know nodes location it require many network protocols and middleware services than depend on the location information of the node. The following are some algorithm in localization in order to find the position of the nodes in wireless sensor networks.

2.1 Centralized versus Distributed Localization Algorithms

Based on the computational organization the localization algorithms are divided into centralized and distributed algorithms. In centralized algorithms the nodes send data to central location where evaluation and location of each node is found and sent back to the nodes. The main draw back is the high communication cost and intrinsic delay. The intrinsic delay increases when there are more nodes in the network so this centralized is not suitable for large networks.

So to decrease the delay and minimize the communication between the senor nodes the distributed algorithm is introduced. Each node finds its location by communicating with neighbor nodes. The distributed algorithm is more robust as the nodes find their position locally by not sending or receiving information from central server which makes it more energy efficient. The drawback of this algorithm as it is more complex to implement due to the limited computational capability of the sensors.

2.2 Range free Versus Range Based Technique

Range-Free techniques use the connectivity information between neighboring nodes to find the position of the nodes whereas Range-based needs ranging information to find the distance between the neighboring nodes. Range-free do not need any additional hardware and use nearer information to find the location of the nodes. On the other hand Range-Based use range measures such as Time of Arrival (ToA), Angle of Arrival (AoA), Received signal strength indicator (RSSI), and Time Difference of Arrival (TDoA) to measure the distance between the nodes to find the position.

2.3 Anchor-based Versus Anchor-free Technique

Sometimes for classification of algorithms external reference nodes are needed called as anchor nodes. They have GPS received installed on them or know their place by eleven manual configurations. When the absolute reference system is being used the other nodes use the reference nodes in order to provide the coordinates.

To coincide with absolute coordinate system the Anchor Based algorithm use anchor nodes to rotate, translate, and even scale the system. In this algorithm at least a minimum number of anchor nodes are required for proper results. The drawback of Anchor-base is that it needs a position system to find the position of the node and if it is not available the algorithm may not function properly. Another drawback is the system needs a GPS receiver mounted as it increases the expense of the system.

Anchor-Free do not require anchor nodes where as it provides only relative node location to find the location of the nodes that reflects the position of the sensor nodes relative to each other.

3, Review of the Recent Techniques of Faults Localization in Sensor Networks

3.1 Localization of Mobile Nodes

Wireless Sensor Networks are essential part of decision making, Object tracking and location awareness system. By using receive signal strength indicator (RSSI) the continuous location of mobile nodes is found with correlated time measurement noise. In the framework of auxiliary particle filtering two approaches are used to deal with correlated measurement noise. First approach is noise augmented state vector and second implements noise de correlation, Multi model auxiliary particle filters (MM AUX-PF) solves the self localization problem of mobile nodes by taking into account the temporal correlation in the measurement noise [1].

To improve better modeling of networks with information-theoretic security constraints will reduce the connectivity of wireless networks in the presence of eavesdroppers. The author is concerned with the previous secure connection from a typical transmitter to the legitimate receivers over fading channels where the unwanted nodes and eavesdroppers are all randomly located. They consider non-colluding and colluding eavesdroppers and the network secure connectivity is derived for both eavesdropper strategies. Secure Wireless Network Connectivity with Multi-Antenna Transmission [4]

improves secure connectivity by forming a directional antenna but not extended to the local to global connectivity

3.2 Anomalies Detection Techniques in WSN

There is a need of increase in automating methods in detecting and diagnosing cells as the complexity of commercial cellular networks grows. A novel integrated detection and diagnosis framework [2] is needed so that it can identify anomalies and find the root cause of the server problems and even smaller degradation. The anomalies are detected based on the monitoring radio measurements and other performance indicators and comparing them to their behavior.

The important concept in redundancy management is to utilize the tradeoff between energy consumptions and the gain in reliability, timeliness and security to maximize the system useful lifetime. The tradeoff is formulated as an optimization problem for dynamically determining the best redundancy level so that the multipath routing is applied for best redundancy level. Novel probability model examine the best redundancy level in terms of path redundancy and source redundancy but trust management does not strengthen fault detection [7].

Anonymous routing protocols used in MANET to hide the node identities and routes from outsiders to provide protection. Anonymous Location-Based efficient routing protocol (ALERT) offers high protection against anonymity at a low cost [8]. It dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes, which is not sturdy in demonstrating comprehensive theoretical results

There will be sometimes problems in deployment of wireless sensor networks while monitoring applications. Sometimes more packet collisions make way to packet losses and retransmission which results in significant overhead costs and latency. Distributed and Scalable scheduling access scheme is introduced so that it reduces the high data loss in data intensive sensor network and also can handle mobility. Distributed and Scalable Time Slot Allocation Protocol makes use of virtual grids that adopt Latin Squares characteristics but fails in achieving the network scalability [9].

3.3 Protocols and Topology in Localization

The process of publishing new code image or suitable commands to sensor nodes is called wireless reprogramming. As WNS is deployed in unfriendly environment so the security is a major issue. While the reprogramming protocols follow centralized approach which may involve base station it is important to support distributed reprogramming where multiple network users can directly reprogram the sensor nodes without involving the base station. Secure and Distributed Reprogramming Protocol (SDRP) eliminates the design weakness by adding 1-B redundant data [3]. Secure a Multi hop Network Programming (SMNP)

protocol through the use of multiple one-way hash chains is shown to be lower in computational, power consumption and communication costs [10].

The security proposed for vehicular networks take as an input centrality measures calculated by mapping the centrality values of the networks to the given road topology [11]. The resulting strategies help locating most valuable or important points in vehicular networks. Thus, optimal deployment of traffic control and security infrastructure is found both in the static and dynamic cases. Distributed cache invalidation mechanism (DCIM) is a client-based cache consistency scheme [12] that is used on top of a previously used architecture for caching data items in mobile ad hoc networks (MANETs). DCIM is a pull-based algorithm that implements adaptive time to live (TTL), piggybacking, and prefetching, and provides near strong consistency capabilities. Cached data items are assigned adaptive TTL values that correspond to their update rates at the data source, where items with expired TTL values are grouped in validation requests to the data source to refresh them.

4, PARAMETRIC ANALYSIS OF SENSOR NETWORK FAULT LOCALIZATION METHODS

Existing Multi model auxiliary particle filters (MM AUX-PF) solves the self localization problem of mobile nodes by taking into account the temporal correlation in the measurement noise. Secure Wireless Network Connectivity with Multi-Antenna Transmission improves secure connectivity by forming a directional antenna. Pseudonym changing at social spots (PCS) strategy attains the verifiable location privacy. PCS develop two anonymity set analytic models to quantitatively investigate the location privacy. Motion Tracking Using Variance-Based Radio Tomography Networks show that the signal strength on a wireless link that travel through space containing moving objects.

Integrated detection and diagnosis framework identify anomalies and find the most probable root cause. Integrated detection and diagnosis framework faces the most complex fault cases on different characteristics impact. Redundancy Management of heterogeneous wireless sensor networks utilizes multipath routing to answer user queries in the presence of unreliable and malicious nodes. Novel probability model examine the best redundancy level in terms of path redundancy and source redundancy.

An Anonymous Location-Based Efficient Routing Protocol (ALERT) in MANET dynamically partitions the network field into zones and randomly chooses nodes in zones as intermediate relay nodes. Distributed and Scalable Time Slot Allocation Protocol makes use of virtual grids that adopt Latin Squares characteristics. Secure and Distributed Reprogramming Protocol (SDRP) eliminates the design weakness by adding 1-B redundant data. Secure a Multihop Network Programming (SMNP) protocol through the use of multiple one-way hash chains. SMNP is shown to be lower in computational, power consumption and communication costs.

Security games for vehicular networks take input centrality procedures calculate by mapping the centrality principles of the car networks to the fundamental road topology. Distributed Cache Invalidation Method provides near strong consistency capabilities do not perform incorporation operation on correct security measures into the system functions.

Methods/Techniques	**Parameters**									
	Location privacy metric	**Localization accuracy**	**Energy efficiency**	**Computational cost**	**Routing overhead**	**Root Cause Analysis**	**Measurement Noise**	**Redundancy Level**	**Execution Time**	**Strong Consistency**
Multi model auxiliary particle filters	**Y**						**Y**			
Multi-Antenna Transmission		**Y**								
Pseudonym changing at social spots	**Y**			**Y**				**Y**		
Radio Tomography Networks	**Y**			**Y**						
Integrated detection and diagnosis framework	**Y**					**Y**				
Probability model				**Y**				**Y**		
Location-Based Efficient Routing Protocol	**Y**			**Y**	**Y**					
Distributed and Scalable Time Slot Allocation Protocol	**Y**								**Y**	**Y**
Secure and Distributed Reprogramming Protocol	**Y**		**Y**	**Y**						

Multihop Network Programming				**Y**		**Y**				
Security games for vehicular networks				**Y**	**Y**					**Y**
Distributed Cache Invalidation Method	**Y**									**Y**

Fig 4.1: Parameters Used in Finding Faults in WSN

Y --- Indicates the usability of parameters in corresponding technique

5, CONCLUSION

In the wireless sensor network the problem faced is finding the position of the nodes, communication between the nodes under limited resources and processing noisy data without any reduction. These faults are found and solved using some of the techniques discussed in this survey. Anchor Free-Movable Topographical Scattered Localization (AF-MTSL) technique makes use of a standard device accelerometer to localize fixed and mobile nodes with each other for effective communication. MTSL technique has flexible communication overhead for both high mobility and low mobility nodes, while inflict lower communication overhead. Self Fault Diagnosis model (SFD) leverages both Composition and Behavioral Model (CBM) and Logic based Backward Analysis (LBA). The novelty results in decoupled architecture where CBM quickly updated independent of LBA, which is often necessary for changing wireless environment and configurations. Similarity Hashing Function and an Identity based Combined Signature allows nodes to check incoming encoded packets, and introduces an efficient mechanism to reduce the computation overhead and protect from effluence attack. Experimental evaluation is measured in terms of fault detection efficiency, communication overhead, average error rate, time consumption and packet loss rate.

6, SCOPE FOR FUTURE EMPHASIS IN FAULT LOCALIZATION TECHNIQUES

Many techniques have been surveyed which need some improvement to make it reliable in the future. Existing Multi model auxiliary particle filters (MM AUX-PF) the connectivity issues occur when localization of both fixed and mobile nodes communicate with each other. Secure Wireless Network Connectivity with Multi-Antenna Transmission will not extend to local to global connectivity. To attain a solution to these drawbacks, topographical scattered localization technique can be used to localize both fixed and mobile nodes for effective communicate with each other. The topographical scattered localization technique in wireless networks could supervise a moving space for every node, and then uses measures to sense any movement of each node.

Integrated detection and diagnosis framework faces the most complex fault cases on different characteristics impact. In Redundancy Management of heterogeneous wireless sensor networks trust management does not strengthen fault detection. To overcome these issues, focus is made on developing self established fault diagnosis for fault detection and diagnosis. Self established fault diagnosis may provide construction of composition and behavioral patterns. The analysis and model description are decoupled so as to easily update for varying configurations and changing network conditions.

Secure and Distributed Reprogramming Protocol fails in integrating with a more reprogramming protocol for proficient distributed reprogramming. Secure Multi-hop Programming may provide lower computational, power consumption and communication costs yet still not able to design privacy model for improved scalability in network programming. To achieve this, privacy approach may able to protect effluence attack against reprogramming protocols based on network coding. It employs a similarity hashing and individuality based aggregate signature allow sensor nodes to check packets on the wing before they accept incoming encoded packets. Similarity hashing provides an efficient mechanism to reduce the computation overhead at each node and to eliminate bad packets quickly.

7, REFERENCES

[1] Lyudmila Mihaylova., Donka Angelova., David R. Bull., and Nishan Canagarajah, "Localization of Mobile Nodes in Wireless Networks with Correlated in Time Measurement Noise," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL 10, NO 1, JANUARY 2011

[2] Peter Szilagyi., and Szabolcs Novaczki., "An Automatic Detection and Diagnosis Framework for Mobile Communication Systems," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 9, NO. 2, JUNE 2012

[3] Daojing He., Chun Chen., Sammy Chan., Jiajun Bu., and Laurence T. Yang., "Security Analysis and Improvement of a Secure and Distributed Reprogramming Protocol for Wireless Sensor Networks," IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 11, NOVEMBER 2013

[4] Xiangyun Zhou., Radha Krishna Ganti and Jeffrey G. Andrews., "Secure Wireless Network Connectivity with Multi-Antenna Transmission," IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, ACCEPTED FOR PUBLICATION., 2010

[5] Rongxing Lu., Xiaodong Lin., Tom H. Luan., Xiaohui Liang., and Xuemin (Sherman) Shen., "Pseudonym Changing at Social Spots: An Effective Strategy for Location Privacy in VANET," IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, VOL. 61, NO. 1, JANUARY 2012

[6] Joey Wilson and Neal Patwari., "See-Through Walls: Motion Tracking Using Variance-Based Radio Tomography Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 5, MAY 2011

[7] Hamid Al-Hamadi., and Ing-Ray Chen., "Redundancy Management of Multipath Routing for Intrusion Tolerance in Heterogeneous Wireless Sensor Networks," IEEE TRANSACTIONS ON NETWORK AND SERVICE MANAGEMENT, VOL. 10, NO. 2, JUNE 2013

[8] Haiying Shen., and Lianyu Zhao., "ALERT: An Anonymous Location-Based Efficient Routing Protocol in MANETs," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 6, JUNE 2013

[9] Chih-Kuang Lin., Vladimir I. Zadorozhny., Prashant V. Krishnamurthy., Ho-Hyun Park, and Chan-Gun Lee., "A Distributed and Scalable Time Slot Allocation Protocol for Wireless Sensor Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 5, APRIL 2011

[10] Hailun Tan., John Zic., Sanjay K. Jha., and Diethelm Ostry., "Secure Multihop Network Programming with Multiple One-Way Key Chains," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 1, JANUARY 2011

[11] Tansu Alpcan., and Sonja Buchegger., "Security Games for Vehicular Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 10, NO. 2, FEBRUARY 2011

[12] Kassem Fawaz., and Hassan Artail., "DCIM: Distributed Cache Invalidation Method for Maintaining Cache Consistency in Wireless Mobile Networks," IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 4, APRIL 2013