ISSN: 2348 - 2117

International Journal of Engineering Technology and Computer Research (IJETCR)
Available Online at www.ijetcr.org
Index Copernicus Value 2016: 69.88
Volume 7; Issue 1; January-February 2019; Page No. 16-22

DECENTRALIZED HYPOTHESIS TESTING IN WIRELESS SENSOR NETWORKS

Payal Vaya, Dr. Bharat Singh Deora

JRN Rajasthan Vidhyapeeth University

Abstract

Wireless sensor networks are prone to node misbehavior arising from tampering by an adversary (Byzantine attack), or due to other factors such as node failure resulting from hardware or software degradation. In this paper, we consider the problem of decentralized detection in wireless sensor networks in the presence of one or more classes of misbehaving nodes. Binary hypothesis testing is considered where the honest nodes transmit their binary decisions to the fusion center (FC), while the misbehaving nodes transmit fictitious messages. The goal of the FC is to identify the misbehaving nodes and to detect the state of nature. We identify each class of nodes with an operating point (false alarm and detection probabilities) on the receiver operating characteristic (ROC) curve. Maximum likelihood estimation of the nodes' operating points is then formulated and solved using the expectation maximization (EM) algorithm with the nodes' identities as latent variables. The solution from the EM algorithm is then used to classify the nodes and to solve the decentralized hypothesis testing problem. Numerical results compared with those from the reputation-based schemes show a significant improvement in both classifications of the nodes and hypothesis testing results. We also discuss an inherent ambiguity in the node classification problem which can be resolved if the honest nodes are in majority.

Key words: Vectors, Testing, Wireless sensor networks, Sensors, Collaboration, Estimation, Maximum likelihood detection

INSPEC: Controlled Indexing

Wireless sensor networks, binary decision diagrams, expectation-maximisation algorithm

INSPEC: Non-controlled Indexing

Reputation-based schemes, wireless sensor networks, decentralized hypothesis testing, misbehaving nodes, node misbehavior, adversary tampering, Byzanthine attack, node failure, hardware degradation, software degradation, binary hypothesis testing, binary decisions, fusion center, fictitious messages, operating point, false alarm, detection probability, receiver operating characteristic curve, maximum likelihood estimation, expectation maximization

INTRODUCTION

Wireless sensor networks (WSNs) consist of a large number of tiny battery-powered sensors that are densely deployed to sense their environment and report their findings to a central processor (fusion center) over wireless links. Due to size and energy constraints, sensor nodes have limited processing, storage and communication capabilities. In a large network of such sensors many nodes may fail due to hardware degradation or environmental effects. While in some cases a faulty node stops operating altogether, in other cases it may be misbehaving and reporting false data as in the case of stuck-at faults.

Wireless Sensor Network (WSN) is the most standard services employed in commercial and industrial applications, because of its technical

Corresponding author: Payal Vaya

development in a processor, communication, and low-power usage of embedded computing devices. The WSN is built with nodes that are used to observe the surroundings like temperature, humidity, pressure, position, vibration, sound etc. These nodes can be used in various real-time applications to perform various tasks like smart detecting, a discovery of neighbor node, data processing and storage, data collection, target tracking, monitor and controlling, synchronization, node localization, and effective routing between the base station and nodes.

Presently, WSNs are beginning to be organized in an enhanced step. It is not awkward to expect that in 10 to 15 years that the world will be protected with WSNs with entree to them via the Internet. This can be measured as the Internet becoming a physical n/w. This technology is thrilling with infinite potential for many application areas like medical, environmental, transportation, military, entertainment, homeland defense, crisis management and also smart spaces.

A Wireless Sensor Network is one kind of wireless network includes a large number of circulating, self-directed, minute, low powered devices named sensor nodes called motes. These networks certainly cover a huge number of spatially distributed, little, battery-operated, embedded devices that are networked to caringly collect, process, and transfer data to the operators, and it has controlled the capabilities of computing & processing. Nodes are the tiny computers, which work jointly to form the networks.

The sensor node is a multi-functional, energy efficient wireless device. The applications of motes in industrial are widespread. A collection of sensor nodes collects the data from the surroundings to achieve specific application objectives. The communication between motes can be done with each other using transceivers. In a wireless sensor network, the number of motes can be in the order of hundreds/ even thousands. In contrast with sensor n/ws, Ad Hoc networks will have fewer nodes without any structure.

Wireless Sensor Network Architecture

The most common WSN architecture follows the OSI architecture Model. The architecture of the WSN includes five layers and three cross layers. Mostly in sensor n/w we require five layers, namely application, transport, n/w, data link & physical layer. The three cross planes are namely power management, mobility management, and task management. These layers of the WSN are used to accomplish the n/w and make the sensors work together in order to raise the complete efficiency of the network. Please follow the below link for: Types of wireless sensor networks and WSN topologies

Characteristics of Wireless Sensor Network

- The consumption of Power limits for nodes with batteries
- Capacity to handle with node failures
- Some mobility of nodes and Heterogeneity of nodes
- Scalability to large scale of distribution
- Capability to ensure strict environmental conditions
- Simple to use
- Cross-layer design

Advantages of Wireless Sensor Networks

- Network arrangements can be carried out without immovable infrastructure.
- Apt for the non-reachable places like mountains, over the sea, rural areas and deep forests.
- Flexible if there is a casual situation when an additional workstation is required.
- Execution pricing is inexpensive.
- It avoids plenty of wiring.
- It might provide accommodations for the new devices at any time.

- It can be opened by using a centralized monitoring.

Applications Used

Area monitoring

In area monitoring, the WSN is deployed over a region where some phenomenon is to be monitored. A military example is the use of sensors to detect enemy intrusion; a civilian example is the geo-fencing of gas or oil pipelines.

Air pollution monitoring

Wireless sensor networks have been deployed in several cities to monitor the concentration of dangerous gases for citizens. These can take advantage of the ad-hoc wireless links rather than wired installations, which also make them more mobile for testing readings in different areas.

Greenhouse monitoring

Wireless sensor networks are also used to control the temperature and humidity levels inside commercial greenhouses. When the temperature and humidity drops below specific levels, the greenhouse manager must be notified.

Machine health monitoring

Wireless sensor networks have been developed for machinery condition-based maintenance (CBM) as they offer significant cost savings and enable new functionalities. In wired systems, the installation of enough sensors is often limited by the cost of wiring.

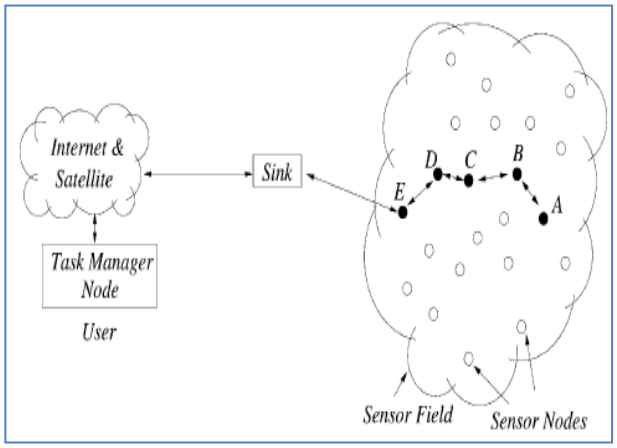
Water/wastewater monitoring

There are many opportunities for using wireless sensor networks within the water/wastewater industries. Facilities not wired for power or data transmission can be monitored using industrial wireless I/O devices and sensors powered using solar panels or battery packs and also used in pollution control board.

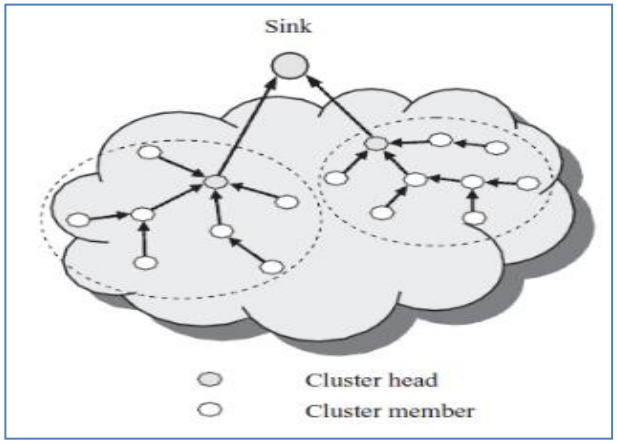
Agriculture

Wireless network frees the farmer from the maintenance of wiring in a difficult environment. Gravity feed water systems can be monitored using pressure transmitters to monitor water tank levels, pumps can be controlled using wireless I/O devices and water use can be measured.

WSN Communication Architecture



Multihop Clustering Hierarchy



Problem Statement

Sensor networks are also vulnerable to tampering. The networks are envisioned to be distributed over a large geographic area with unattended sensor nodes which may be captured and reprogrammed by an adversary. An adversary can also deploy its own sensor nodes to transmit false data in order to confuse the fusion center (FC). Sensors under an adversary's control are often referred to as Byzantine nodes. In binary hypothesis testing, in order to lower their bandwidth requirement and energy expenditures, the sensors often make a local

decision regarding the state of the hypothesis and only send their binary decision to the FC.

REVIEW OF LITERATURE

It is assumed that through collaboration, the Byzantine nodes are aware of the true hypothesis. The authors formulate the problem in the context of Kullback–Leibler divergence and obtain optimal attacking distribution for the Byzantine nodes using a water-filling procedure.

Considered data fusion schemes in a network under Byzantine attack and propose techniques for identifying the malicious users. Considered adding stochastic resonance noise at the honest and/or Byzantines in order to enhance the detection performance.

Cooperative spectrum sensing in cognitive radio networks (CRN) is another example of decentralized hypothesis testing where the secondary (unlicensed) users make a binary decision on whether a channel is vacant of the primary (licensed) user or not, and transmit that decision to the FC. The FC then processes the received data from all the secondary users and decides on the state of the channel. This problem is identical to the classical decentralized detection and recently several papers have considered cooperative spectrum sensing in the presence of Byzantine attacks (spectrum sensing data falsification).

Sequential probability ratio test is modified via a reputation-based mechanism in order to filter out the false data and only accept reliable messages.

A method is presented to detect the Byzantine nodes based on how their transmissions compare with those expected from honest nodes. These approaches are often categorized as reputation-based fusion rules.

EXISTING SYSTEM

- Data fusion schemes in a network under Byzantine attack and propose techniques for identifying the malicious users.
- Adding stochastic resonance noise is considered at the honest and/or Byzantines in order to enhance the detection performance.
- Cooperative spectrum sensing in cognitive radio networks (CRN) is a decentralized hypothesis testing where the secondary users make a binary decision on whether a channel is vacant of the primary user or not, and transmit that decision to the FC. The FC then processes the received data from all the secondary users and decides on the state of the channel.
- Sequential probability ratio test is modified via a reputation-based mechanism in order to filter out the false data and only accept reliable messages.

Disadvantages

In cooperative spectrum sensing it may have more than one class of unreliable nodes.

Therefore the proposed algorithms for CRNs may not always be scalable for WSNs.

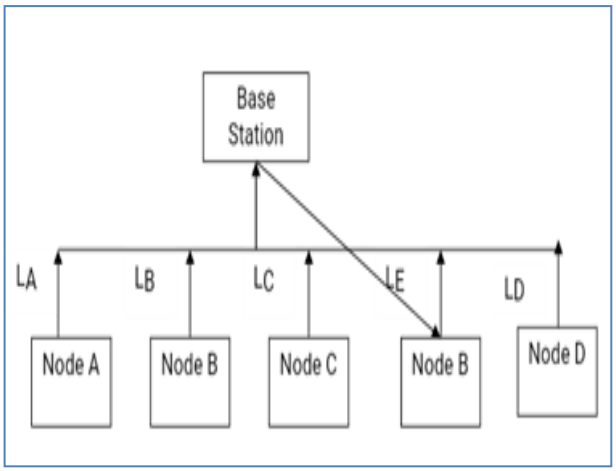
PROPOSED SYSTEM

- Having received the messages from all the nodes, the FC will detect the hypothesis using a judicious decision rule
- It is assumed that there may be more than one class of misbehaving nodes.
- To show that from the point of view of the FC each class can be identified with a (operating) point on the receiver operating characteristic (ROC) that corresponds to the decision rule of the sensor nodes in that class.
- First estimate the operating points of each class.
- To detect the class identity of each node and also detect the hypothesis vector.

Advantages

- Scalable
- Efficient
- Identify more than one malicious node

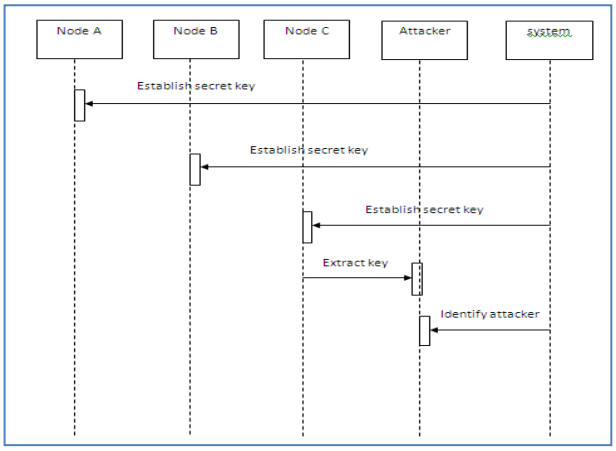
SYSTEM ARCHITECTURE



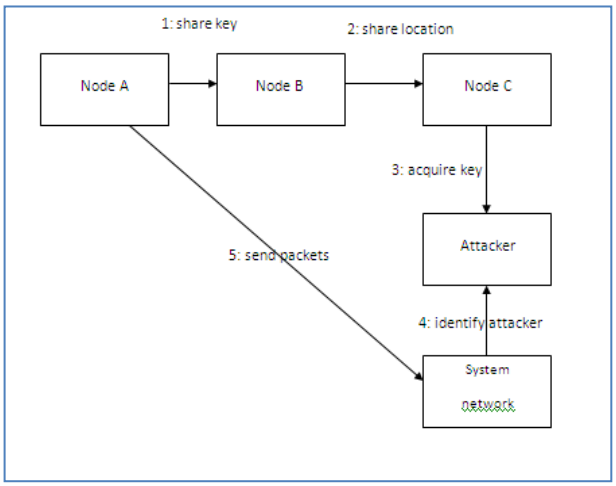
UML DIAGRAM

USE CASE DIAGRAM

SEQUENCE DIAGRAM



COLLABORATION DIAGRAM



SYSTEM OVERVIEW

MODULES

NORMAL NODE

Normal node in wireless sensor network is constructed in such a way that, it has its own id and key. The sensor node forwards the data to base station. Every mobile sensor node's movement is physically limited by the system configured maximum speed.

ATTACKER NODE

Attacker node is the replica node, which is created by adversary; this is known as replica node attacks. A mobile replica node $u^{|}$, which has the same ID and secret key of normal mobile node u. An adversary creates replica node by first compromising node u and extracts all secret keys from it. Then prepares a new node, sets the same ID as normal node and loads normal node's secret key.

CLAIM GENERATION

Each and every mobile sensor node u generates location claim Cu = {u||Lu||T||Sigu} and sends it to a neighboring node v, where u, is the node identity, Lu is the Location, T is the Time and Sigu is the signature generated by node u's private key. Each time a mobile sensor node u moves to a new location, it first discovers its location Lu. Base station receive location claim from the mobile sensor nodes. Upon receiving a location claim, the base station verifies the authenticity of the claim with the public key of node u and discards the claim if it is not authentic.

ATTACK DETECTION

Attack detection is performed using hypothesis testing. As the wireless network is deployed as clusters, the attackers are identified in each and every cluster separately. Under the attack detection, the victim and the attacker are using the same ID to transmit data packets.

DETECTION OF MULTIPLE ATTACKER

Attack detection is identified as statistical significance testing problem, where the null hypothesis is: H0: normal (no attack). In attack detection phase, the same node identity is partitioned into 2 clusters (i.e. K = 2) no matter how many attackers are using this identity. Initially the attacker 'A' is given a value 0.

Whenever, the attackers are indentified, the value of A is incremented.

SOFTWARE REQUIREMENT SPECIFICATION

Functional requirements

1. Normal node in wireless sensor network is constructed in such a way that, it has its own id and key.

2. Sensor node forwards the data to base station

3. Every mobile sensor node's movement is physically limited by the system configured maximum speed.

4. Attacker node is the replica node, which is created by adversary; this is known as replica node attacks.

5. A mobile replica node u^{l}, which has the same ID and secret key of normal mobile node u.

6. Victim and the attacker are using the same ID to transmit data packets

7. Attack detection is identified as statistical significance testing problem, where the null hypothesis is: H0: normal (no attack).

8. For each user u select a set su of up to m distinct items from u's search history in S

NON FUNCTIONAL REQUIREMENTS

Table 1:

Area	Codes & Standards / Realistic Constraints
Economic	This project is very economical as it only depends on the software components to be downloaded from the internet
Performance	This project Performance is high when compared with other file transfer mechanisms
Reliability	This project provides reliability because of the efficient usage of TCP protocol
Security	This project focuses on applying security concepts for authenticating the application.
Manufactura bility	This project can be easily replicated. This requires complete schematics, complete and documented code listings, JSP, produced in a file format accessible by software available at JAVA

RESULTS

Having received the messages from all the nodes, the FC will detect the hypothesis using a judicious decision rule

It is assumed that there may be more than one class of misbehaving nodes. To show that from the point of view of the FC each class can be identified with a (operating) point on the receiver operating characteristic (ROC) that corresponds to the decision rule of the sensor nodes in that class. First estimate the operating points of each class. For a fixed hypothesis vector, formulate this problem as a maximum likelihood estimation problem with latent variables which correspond to the class identity of the nodes. This problem is then solved using the expectation maximization algorithm. Following this step to detect the class identity of each node and also detect the hypothesis vector.

Testing

After finishing the development of any computer based system the next complicated time consuming process is system testing. During the time of testing only the development company

can know that, how far the user requirements have been met out, and so on. Software testing is an important element of the software quality assurance and represents the ultimate review of specification, design and coding. The increasing feasibility of software as a system and the cost associated with the software failures are motivated forces for well planned through testing.

CONCLUSION

The problem of decentralized detection is considered in the presence of one or more classes of misbehaving nodes. The fusion center first estimates the nodes' operating points (false alarm and detection probabilities) on the ROC curve and then uses this estimation to classify the nodes and to detect the state of nature. This problem is solved in the framework of expectation maximization algorithm. Numerical results are presented that show the proposed algorithm significantly outperforms the reputation-based methods in classification of the nodes as well as the detection of the hypotheses. The estimated operating points are compared to the Cramer–Rao lower bound which shows the efficacy of the proposed method.

REFERENCES

1. M. Franceschelli, A. Giua, and C. Seatzu, "Decentralized fault diagnosis for sensor networks," in Proc. IEEE Int. Conf. Autom. Sci. and Eng., 2009 (CASE 2009), Aug. 2009, pp. 334–339.
2. P. Varshney, Distributed Detection and Data Fusion, 1st ed. New York: Springer-Verlag, 1997.
3. S. Marano, V. Matta, and L. Tong, "Distributed inference in the presence of Byzantine sensors," in Proc. 40th Asilomar Conf. Signals, Syst. and Computers, 2006 (ACSSC '06), Oct. 29–Nov. 1, 2006, pp. 281–284.
4. S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," IEEE Trans. Signal Process., vol. 57, no. 1, pp. 16–29, Jan. 2009.
5. M. Abdelhakim, L. E. Lightfoot, and T. Li, "Reliable data fusion in wireless sensor networks under Byzantine attacks," in Proc. Military Commun. Conf., 2011 (MILCOM 2011), Nov. 2011, pp. 810–815.
6. M. Gagrani, P. Sharma, S. Iyengar,V.Nadendla, A. Vempaty, H. Chen, and P. Varshney, "On noise-enhanced distributed inference in the presence of Byzantines," in Proc. 49th Annu. Allerton Conf. Commun., Control, and Comput. (Allerton), 2011, Sep. 2011, pp. 1222–1229.
7. R. Chen, J.-M. Park, and K. Bian, "Robust distributed spectrum sensing in cognitive radio networks," in Proc. IEEE 27th Conf. Computer Commun. (INFOCOM 2008), Apr. 2008, pp. 1876–1884.
8. A. Rawat, P. Anand, H. Chen, and P. Varshney, "Countering Byzantine attacks in cognitive radio networks," in Proc. 2010 IEEE Int. Conf. Acoust. Speech and Signal Process. (ICASSP), Mar. 2010, pp. 3098–3101.
9. P. Anand, A. Rawat, H. Chen, and P. Varshney, "Collaborative spectrumsensing in the presence of Byzantine attacks in cognitive radio networks," in Proc. 2010 2nd Int. Conf. Commun. Syst. and Netw. (COMSNETS), Jan. 2010, pp. 1–9.
10. M. Abdelhakim, L. Zhang, J. Ren, and T. Li, "Cooperative sensing in cognitive networks under malicious attack," in Proc. 2011 IEEE Int. Conf. Acoust., Speech and Signal Process. (ICASSP), May 2011, pp. 3004–3007.