IJREAT International Journal of Research in Engineering & Advanced Technology, Volume 2, Issue 2, Apr-May, 2014
ISSN: 2320 – 8791 (Impact Factor: 1.479)
www.ijreat.org

Transmission of Data between Sensors by Devolved Recognition

Ms. K. P. Geethanjali[1], Ms. R. Vasanthi[2]

[1, 2]PG Scholar, Department of Computer Science and Engineering, Dr. Pauls Engineering College, Villupuram - 605 109

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. Each sensor has a time out period and listens to messages sent by respective nodes before the time out expires. Sensor nodes whose sensing area is not fully covered when the deadline expires decide to remain active for the considered round and transmit an activity message announcing it. All the sensors will keep the list of devices which communicates at a time. Here, each sensor communicates with all the sensors on the network and/ or with neighbor sensors. Sensors with low time-period watch all the neighbors and if they are available, sensor turns to sleep, and all the devices will assigned to particular neighbor sensor. Daisy chain architecture and Multi-Sensor Fusion Algorithm is used to solve this problem. Objective is that while transmitting the data from one node to another and if any problem comes, sensors will automatically find the problem and it will fix.

Index Terms *–Network Security, Byzantine attack, decentralized hypothesis testing, sensor node classification, wireless sensor networks.*

1. INTRODUCTION

Wireless sensor networks 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 [1].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. The problem of decentralized detection in the presence of Byzantine nodes has been investigated [2]. It is assumed that through collaboration, the Byzantine nodes are aware of the true hypothesis. In [3], data fusion schemes in a network under Byzantine attack and propose techniques for identifying the malicious users.

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).

Malicious users may send false data in order to gain unfair access to the channel, others may be sending incorrect data due to the malfunctioning of their sensing terminal. We should also point out that while a collaborative CRN may consist of at most tens of radios, a sensor network may comprise of hundreds or thousands of nodes. Therefore the proposed algorithms for CRNs may not always be scalable for WSNs. For a fixed hypothesis vector, we formulate this problem as a maximum likelihood estimation problem with latent variables which correspond to the class identity of the nodes.

2. RELATED WORKS

Byzantine attacks in wireless sensor networks compromisesthe active sensors to send false information. One effective method to combat with Byzantine attacks is the q-out-of-m scheme, where the sensing decision is based on q sensing reports out of m polled nodes. It is simple and effective. Cooperative sensing in cognitive networks under Spectrum Sensing Data Falsification attack (SSDF) [4] in which malicious users can intentionally send false sensing information. One effective method to deal with the SSDF attack is the q- out-of-m scheme, where the sensing decision is based on q sensing reports out of m polled nodes. For a fixed percentage of malicious users, the detection accuracy increases almost exponentially as the network size increases. The problem of fault diagnosis for sensor networks which examine faults involves an anomalous behavior of the sensor. It provides heuristics to actively diagnose faults and recover the nominal behavior. The main contribution of this work is: 1) A classification of faults in a sensor network that disrupt the consensus dynamics. 2) A heuristic to classify suspected behavior of the nodes when a fault is likely. The noise-enhanced distributed detection problem in the presence of Byzantine (malicious) nodes suitably adds stochastic resonance noise [5]. Two metrics are used. 1) The minimum number of Byzantines (α_{blind}) needed to blind the fusion center as a security metric. 2) The Kullback – Leibler divergence (D_{KL}) as a detection performance metric. The problem of fusing decisions transmitted over fading channels [6] in a wireless sensor network is carried. A new likelihood ratio (LR)-based fusion rule requires only the knowledge of channel statistics instead of instantaneous CSI. EGC is a very good choice with low or medium SNR. Collaborative (or distributed) spectrum sensing [7] has been shown to have various advantages in terms of spectrum utilization and robustness in cognitive radio networks (CRNs).The data fusion scheme is a key component of collaborative spectrum sensing. The problem of binary hypothesis testing is considered in a bandwidth-constrained densely populated low-power wireless sensor network operating over insecure links. Observations of the sensors are quantized and encrypted before transmission. The intended (ally) fusion center (AFC) is aware of the encryption keys (probabilities) while the unauthorized (third party) fusion center (TPFC) is not [8].

3. EXISTING SYSTEM

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. 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.

- In existing method, sensors are not in a proper contact with its neighbor pair. If the time-out period is over for a sensor, it will go to sleep without any warnings.
- This leads to collision and data loss. Here, resources are not using in proper.
- For dense networks, fails to cover the area reasonably with a connected set of active nodes. Nodes may not know which sensor currently communicates with it.
- EM Algorithm was used.

4. PROPOSED SYSTEM

In proposed scheme, set of sensors transmits a highly compressed summary of its observations (a binary message) and subsets of the sensors to both (star and parallel) transmit their messages to the fusion center.

The daisy chain architecture performs no better than a star architecture with the same number of sensors and observations. The number of sensors in the first and the second stage of the daisy chain architecture is the same. Here hypothesis vector algorithm is used.

Advantages of Proposed System are

- Sensors have admin, hence no malicious users.
- Notification shows which sensor is communicated with which node.
- Daisy chain is simple and scalable.
- The user can add more nodes anywhere along the chain.

4.1 User Authentication

To share the information from one node to another node we have to access the user authentication. Other than Admin no one can access the sensor process. The secured state helps us to do the transmission without any hacking the system. The path of each system will be allocated by the authenticated user only.

4.2 Sensor Communication

Sensor communication is process of data sharing between two sensors. Fast transmission can be occurred with the sensor communication. Switching of communication between each sensor can be done in easier way. Accuracy of data transmission is excellent. There are two ways in Sensor Communication one is Dual and the other is Full. In Dual, the node to node data transfer will be done but we can't able to know which sensor is connected to which node. In Full way communication, the same data transfer will be done but we can able to know which sensor is connected to which node.

4.3 Sharing

In this module, data is transmitted form one node to another then the sensor will be activated. If again the data transmitted form the second node to the third node and if the first sensor gets deactivated, automatically the second sensor will be activated.

4.4 Works of Sensor

First the sensors are created. After creating the sensors the sensing range is viewed. All can also see the communication range in this module. Identifying the sensor range plays an important role for linking the sensors. Once the sensor is made on then it starts to identify the availability of neighboring sensor. If the neighboring sensor is in on-state then communication between the two sensors according to the path ordered by the authentication user. If the sensor identifies the off-state then it starts to save the datas in particular memory location such that when the sensor identifies the on-state then it begins the data sharing.

5. SYSTEM MODEL

A **daisy chain** is an interconnection of computer devices or sensor nodes in series, one after the other. In personal computing, "daisy-chainable" interfaces include Small Computer System Interface and FireWire, which allow computers to communicate with hardware such as disk drives, tape drives faster and more flexibly than previous interfaces. Daisy chain is simple and scalable.

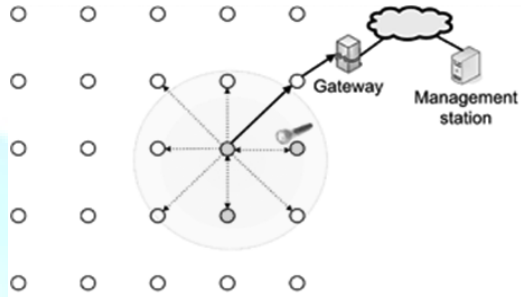

Figure1: System architecture

A **fusion center** is an information sharing center. The fusion process is an overarching method of managing the flow of information and intelligence across levels and sectors of government to integrate information for analysis. That is, the process relies on the active involvement of state, and local enforcement agencies and sometimes on non-law enforcement agencies (e.g., private sector) to provide the input of raw information for intelligence analysis.

A **gateway** is a link between two computer programs allowing them to share information and bypass certain protocols on a host computer.A gateway acts as a portal between two programs allowing them to share information by communicating between protocols on a computer or between dissimilar computers.

A **sensor** is a converter that measures a physical quantity and converts it into a signal which can be read by an observer or by an instrument. A sensor is a device, which responds to an input quantity by generating a functionally related output usually in the form of an electrical or optical signal.

6. PROPOSED MODEL EVALUATION

We evaluate the performance of the proposed method referred to as maximum- likelihood classifier (MLC) and also compare our results with the reputation-based classifier (RBC) algorithm. In RBC when the network parameters (e.g., the nodes' operating points) are known, the optimal -out-of- rule can be computed.

However, when the FC is not aware of all the network parameters as is the case here, majority rule has been used here for our comparisons. For example by setting a threshold on the probability of misclassifying the honest nodes as Byzantines. Moreover, if the fraction of honest nodes is known then can be set to minimize the probability of classification error. In our case, however, the FC is not aware of the fraction of honest nodes. Therefore we set the threshold. For this choice of the probability that an honest node is misclassified as Byzantine is the same as the probability that a Byzantine node is misclassified as honest. Other values of the threshold can favor the classification of honest nodes as Byzantines or vice versa. Simulation results are obtained from at least independent trials. The EM algorithm is assumed to have converged when. Moreover, to overcome the ambiguity of the counterpart networks, we assume that the honest nodes are in majority. This implies that for a network consisting of two classes the break down point of the algorithm is at 50%. The number of possible hypothesis vectors is too large to evaluate exhaustively. Therefore in these cases it is assumed that during the observation period there is at most one change in the hypothesis vector which may occur at random anywhere from time 2 to T-1.

Table I-Class Parameters Of Each Setof Operating Points

Set	p_f	p_d	π
OP1	0.1	0.9	0.6
	0.9	0.3	0.4
OP2	0.2	0.7	0.6
	0.9	0.15	0.4
OP3	0.2	0.7	0.4
	0.9	0.15	0.15
	0.9	0.9	0.2
	0.05	0.05	0.25

7. CONCLUSION

The problem of decentralized detection in the presence of one or more classes of misbehaving nodes is considered in this work. 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. Sensor nodes whose sensing area is not fully covered when the deadline expires decide to remain active for the considered round and transmit an activity message announcing it. All the sensors will keep the list of devices which communicates at a time. Here, each sensor communicates with all the sensors on the network and/ or with neighbor sensors. Sensors with low time-period watch all the neighbors and if they are available, sensor turns to sleep, and all the devices will assigned to particular neighbor sensor. This method is robust in terms of high area coverage with a reasonable amount of active sensors and connectivity preservation despite message losses. This problem is then solved using the daisy architecture and Multi-Sensor Fusionalgorithm to detect the class identity of each node and also to detect the hypothesis vector. Security is provided for node transmission without congestion in the network and having interconnection with neighboring sensors so that data lose and collusion can be reduced.

REFERENCES

[1] Franceschelli. M, Giua. A, and Seatzu. C (2009) , "Decentralized fault diagnosis for sensor networks," in Proc. IEEE Int. Conf. Autom. Sci. and Eng., (CASE), Aug, pp. 334–339.

[2] S. Marano, V. Matta, and L. Tong, "Distributed detection in the presence of Byzantine attacks," IEEETrans. Signal Process., vol. 57, no. 1, pp. 16–29, Jan. 2009.

[3] Abdel hakim. M, Lightfoot. L. E, and Li. T (2011), "Reliable data fusion in wireless sensor networks under Byzantine attacks," in Proc. Military Commun. Conf., (MILCOM), Nov, pp. 810–815.

[4] Abdel hakim. M, Zhang. L, Ren. J, and Li. T (2011), "Cooperative sensing in cognitive networks under malicious attack," in Proc. IEEE Int.Conf. Acoust., Speech and Signal Process. (ICASSP), pp. 3004–3007.

[5] Gagrani. M, Sharma. P, Iyengar. S, Nadendla. V, Vempaty. A, Chen.H, and Varshney. P (2011), "On noise-enhanced distributed inference in the presence of Byzantines," in Proc. 49th Annu.Allerton Conf. Commun., Control, and Comput.(Allerton), Sep., pp. 1222–1229.

[6] Niu. R, Chen. B and Varshney. P (2006), "Fusion of decisions transmitted over Rayleigh fading channels in wireless sensor networks," IEEE Trans.Signal Process., Mar., vol. 54, no. 3, pp. 1018–1027.

[7]Rawat.A, Anand. P, Chen. H and Varshney.P (2010), "Countering Byzantine attacks in cognitive radio networks," in Proc. IEEE Int. Conf. Acoust.Speech and Signal Process. (ICASSP), Mar, pp.3098–3101.[[[[['']=

[8] Soosahabi. R and Naraghi-Pour.M (2012), "Scalable PHY-layer security for distributed detection in wireless sensor networks," IEEE Trans. Inf.Forensics Security, vol. 7, no. 4, pp. 1118–1126, Aug.