Asian Journal of Computer Science and Technology (AJCST)
Vol.2.No.2 2014 pp1-6
available at: www.goniv.com
Paper Received :05-03-2014
Paper Published:28-03-2014
Paper Reviewed by: 1. John Arhter 2. Hendry Goyal
Editor : Prof. P.Muthukumar

IMPROVING NETWORK PERFORMANCE AND SECURITY IN WIRELESS SENSOR NETWORKS BY USING DECENTRALIZED HYPOTHESIS TESTING

B.Karthiga, Ms.R. Sharmila
A.S.Nagar,Elupatti,Thanjavur,India.
bkarthigacse@gmail.com, sharmi_2457@yahoo.com

ABSTRACT

In wireless sensor networks due to its wireless dynamic nature and open medium the network is vulnerable to node misbehaviour arising from tampering by an adversary (byzantine attack) or due to some other factors such as node failure. Its results are software or hardware degradation. In this consider that a fraction of the monitoring sensors are compromised by an adversary. These compromised sensors are captured and reprogrammed to transmit fictitious messages in order to confuse the fusion centre. The binary hypothesis testing is used in the fusion centre. In Binary hypothesis testing, honest nodes aretransmit their binary decisions and the misbehaving(byzantine)nodes are transmit fictitious messages. The goal of the fusion centre is to identify the presence of misbehaving nodes and also identify the state of nature. Then the fusion centre estimates the nodes operating points on the receiver operating characteristic (ROC) curve. The estimation of the nodes operating point is solved by using the expectation maximization (EM) algorithm. The result of the EM algorithm is used to classify the nodes and also to solve the byzantine nodeproblem. The proposed weighted majority algorithm is used to identify the reliable path for the data transmission thereby improving the network performance and security.

Index Terms- Byzantine attack, Wireless senor networks, Binary hypothesis testing, Expectation Maximization

1. INTRODUCTION

Wireless sensor networks (WSNs) consist of a number of sensor nodes, in that the nodes are report theinformation to a fusion center over wireless links. Sensor nodes have limited storage, processing and communication capabilities due to its size and energy constraints. Due to environmental effects or hardware degradationthe sensor nodes may fail in a large network. In this situation, some cases afault node stops its operation and in some other cases sensor nodes aremisbehaving and reporting false data to the fusion center. Furthermore, the wireless transmission medium ismakes possible for the attacker to extract information fromsensor transmissions because it is more vulnerable to eavesdropping. As a result, the adversary can also deploy its own sensor nodes aimed at jamming the honest nodes transmissionsor in order to confuse the fusion center transmit false data.

A. Byzantine Attack

Wireless sensor networks aremore vulnerable to tampering.The networks are envisioned to be distributed over anarea, the fraction of sensor nodes are compromised by an adversary. Then these compromised nodes are captured andreprogrammed by an adversary and also in order to confuse the fusion center adversaries deployits own nodes to transmit false data. Inthis consider the wireless sensor network is designed which undergoes a Byzantine attack in that a fraction ofsensor nodes cooperatively transmit

fictitious messagesin order to impair thecapability of the fusion center.Thus in the network, the sensor nodeswhich is under an adversary's control are referred as Byzantine nodes. This type of attack is named as a byzantine attack.

2. RELATED WORK

The decentralized detection problem is investigated by severalauthors in the presence of Byzantine nodes [3] [4][12][15]. In cognitive radio networks (CRN), Cooperative spectrum sensing isanother example of decentralized hypothesis testing. In this secondaryusers are unlicensed users, theseusers make a binary decision based on channel of the primary (licensed) user is vacant or not and then transmit that decision to the fusion center. Then thereceived data are processes at the fusion center from all the secondary users and then decides the channel state. It is similar to the classicaldecentralized detection problem. Recently,cooperative spectrum sensing is considered in the presence of Byzantineattacks (spectrum sensing data falsification) in several papers [2][5][7]-[10][14].

In order to filter out the false data, in [14] sequentialprobability ratio test is modified via a reputation-basedmechanism and accept onlyreliablemessages. In order to identifythe Byzantine nodes and strategies for best fusion rule in [7] the authors present a scheme.In [12], it is assumed that the Byzantine nodes are aware about the true hypothesis. In the context of Kullback–Leibler divergence the authors formulate the problem and by using a water-filling procedure obtain optimal attacking distribution for the Byzantine nodes. In [3], network under Byzantine attack the authors consider data fusion schemes and propose techniques for identifying the malicious users. In order to enhance the detection performance the authors consider adding stochastic resonance noise [4] at the honest and/or Byzantine nodes.

In [6], a method is presented based on how byzantine nodes transmissions compare with those expected from honest nodes in order to identify the Byzantine nodes. These approaches are categorized asreputation-based fusion rules [7], [19].Then authors note that also have more than one class of unreliable nodes in cooperativespectrum sensing. In order to gain unfair access to the channel some malicious users may send false data and also due to the malfunctioning of their sensing terminal others may be sending incorrect/falsedata.

In this point out that a collaborative cognitive radio network mayconsist of at most tens of radios, a sensor networkmay consist of hundreds or thousands of nodes. Therefore the proposed methodsof CRNs may not be scalable always for wireless sensor networks.However, in the cooperative spectrum sensing in CRNs is also applicable by this proposed method.

3. TECHNIQUES

A. Binary Hypothesis Testing

Binary hypothesis testing is used in the fusion center. The binary hypothesis testing is identified the presence of misbehaving nodes, where the honest nodestransmit their binary decisions and themisbehaving nodes transmit fictitious messages to the fusion center. In binary hypothesis testing, the sensor nodes frequently make a local decision regarding the state of the hypothesis in order to lower their bandwidth requirement and energy expenditures and then only send their binary decision to the fusion center.

Then the fusion center will identify the presence of misbehaving nodesfrom the received messages of all the nodes in the network. The binary decision may be zero or one. The binary decision zero indicates the node is in inactive state and binary decision one indicates the node is in active state. The goal of the fusion center is to identify the presence of misbehaving nodes and also to identify the state.

B. Receiver Operating CharacteristicCurve

The receiver operating characteristic curve is used to estimate the operating points of the nodes. In this show that each class of nodes can be identified with an operating point on the receiver operating characteristic curve from the point of view of the fusion center that corresponds to the sensor nodes decisionin that class.

C. Expectation Maximization Algorithm

The expectation maximization algorithm is used to solve the problem of byzantine attack in the presence of misbehaving nodes. In the network, estimate the maximum likelihood of the nodes operating points is formulated and then solved using the expectation maximization algorithm.The resultof the expectation maximizationalgorithm is thenused to classify the nodes and to solve the byzantine node problem. It shows a significant improvement in bothhypothesis testing results and classification of the nodes.The

expectation maximization algorithmshown is guaranteed to increase the log-likelihood functionfor every update[22].Thus using the expectation maximization algorithm solved the byzantine attack problem thereby improves the security in the wireless sensor networks.The expectation maximization algorithmissignificantly outperforms in detection of the hypotheses and classification of the nodes. Moreover the proposed algorithm is works faster.

D. Weighted MajorityAlgorithm

The weighted majority algorithm is used to find the reliable path in the wireless sensor network. The reliable path is identified during the data transmission between the numbers of nodes. In weighted majority algorithm identify the transmission path which depends upon the node path length.Based on the node path length identify the reliable pathfor every data transmission between the nodes.

The reliable path is chosen due to avoid the traffic during data transmissionbetween the numbers of nodes in the network. So the data transmissions take place without any delay. Thus depends upon the weight of the node path length identify the reliable path for the data transmissions.Thus the proposed weighted majority algorithm improves the network performance during data transmissions in the wireless senor networks.

4. SYSTEM MODEL

Consider the wireless sensor network consisting of number of nodes which undergoes byzantine attack. Therefore the network is in the presence of number of byzantine nodes. Thus in the wireless sensor network the honest nodes are transmit their binary decision and the byzantine nodes are transmit the fictitious messages to the fusion center. This is shown in the fig. 1. Then implement the binary hypothesis testing in the fusion center in order to identify the presence of misbehaving nodes in the network. Then estimate the operating points of the nodes on the receiver operating characteristic curve. This is shown in the fig.2. The expectation maximization algorithm is used to classify the nodes and solve the byzantine node problem and then using the weighted majority algorithm to identify the reliable path for the data transmissions. This isshown in the fig.3. Thereby improve the network performance and security in the wireless sensor network.

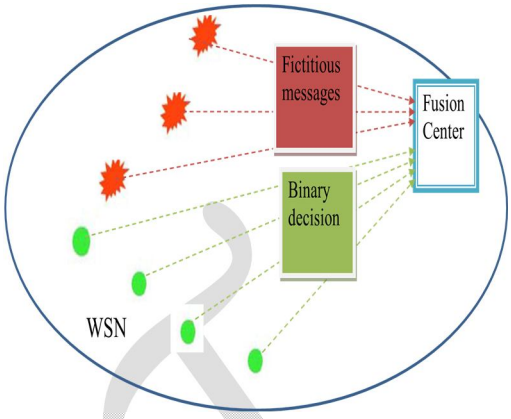

Figure. 1. WSN in the presence of byzantine attacks

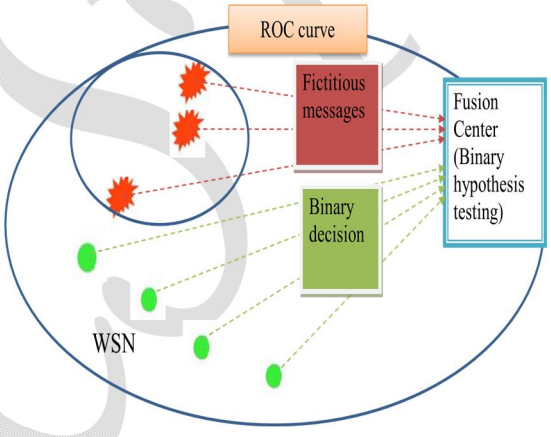

Figure 2. Estimate the operating points of byzantine nodes

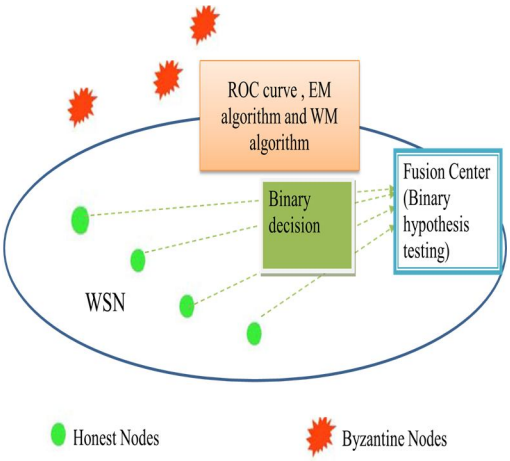

Figure 3. Byzantine nodes are removed in WSN

5. .PERFORMANCE EVALUATION

In this section discuss the simulation results of the proposed system. The purpose of the simulation is to evaluate the performance, security and detection performance of the wireless sensor network.

A. Simulation Setup

Simulate the wireless sensor network as create the number the nodes, in that 50 nodes are honest nodes and 10 to 50 nodes are byzantine nodes which are distributed randomly. Then select the cluster header for the number of nodes in the network. Then simulate the wireless sensor network undergoes the byzantine attack.

B. Simulation Results

i)*In Performance*

Here analyze the performance to verify the effectiveness of the proposed method. In this the number of user are increases from value 50 to 300. By using the proposed method the performance is not decrease as number of users are increases. It gradually maintains the network performance and then improves its performance by choosing the reliable path in the wireless sensor network. It is shown in fig.1.

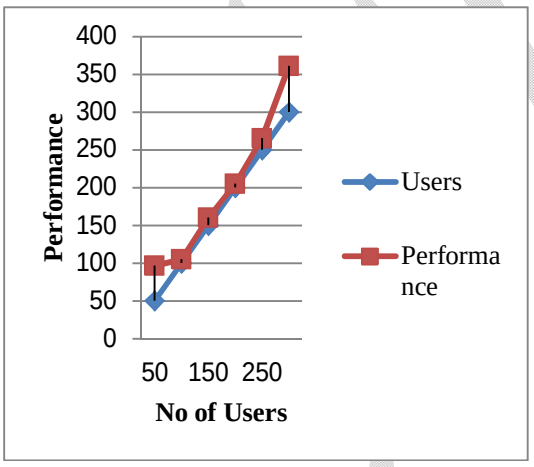

Figure. 1. Number of users versus Performance

ii) *In Security*

Here evaluate the security of the wireless sensor network due to the byzantine attack. In this first identify the presence of byzantine nodes and then remove the byzantine nodes in the wireless sensor network. In the fig. 2 shows as the number of users increases from the value 10 to 50. In this case the security of the wireless sensor network is in constant value 100. Thus it does not degrade the security of the network. By using the proposed method the number of users increases in the wireless sensor network it improves the security and maintains the security of the network.

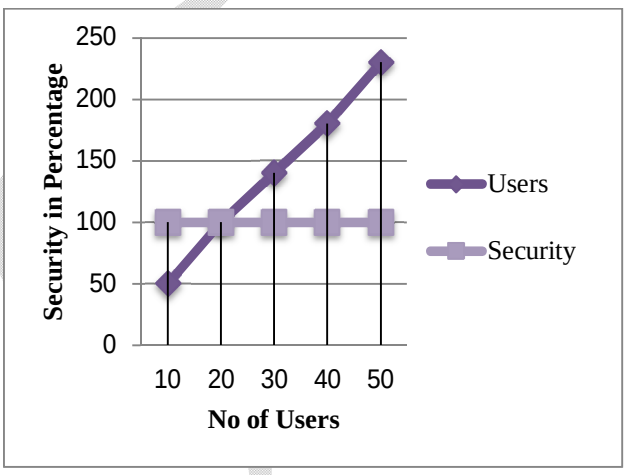

Figure. 2. Number of users versus Security

iii)*In Detection Performance*

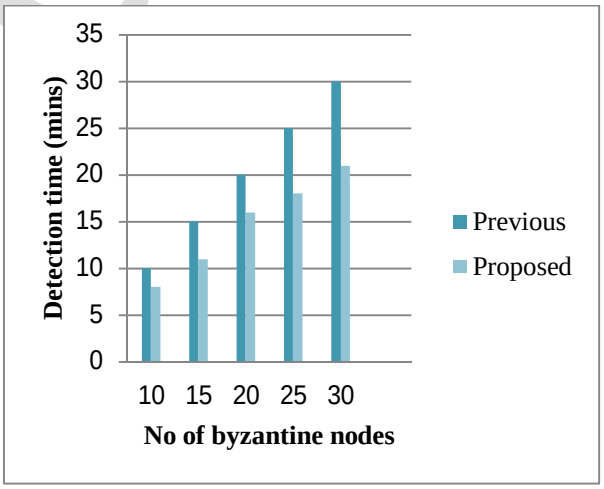

Figure. 3. Previous method versus Proposed method

Here evaluate the detection time in the wireless sensor network. The comparative result of previous

method versus proposed method is shown in fig.3. In this the number of byzantine nodes increases from value 10 to 30. Then the detection time of the previous method and the proposed method is shown in the graph as the number of byzantine nodes increases up to 30. In this comparative results show the detection time is reduced.

6. CONCLUSION

In this paper, consider the problem of byzantine attack in the presence of number of misbehaving nodes in the wireless sensor network. The fusion center estimate the operating points of the nodes on the ROC curve based on the result of the binary hypothesis testing. Then expectation maximization algorithm is used to solve the byzantine attack problem arise in the wireless sensor networks. The weighted majority algorithm is used to identify the reliable path for the data transmission between the nodes. Thereby improves the performance and security in the wireless sensor network.

REFERENCES

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

[2] F. Penna, Y. Sun, L. Dolecek, and D. Cabric, "Detecting and counteracting statistical attacks in cooperative spectrumsensing," IEEE Trans.Signal Process., vol. 60, no. 4, pp. 1806–1822, Apr. 2012.

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

[4] 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.

[5] 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.

[6] A. Vempaty, K. Agrawal, H. Chen, and P. Varshney, "Adaptive learning of Byzantines' behavior in cooperative spectrum sensing," in Proc. 2011 IEEE Wireless Commun. and Network. Conf. (WCNC), Mar. 2011, pp. 1310–1315.

[7] A. Rawat, P. Anand, H. Chen, and P. Varshney, "Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks," IEEETrans. Signal Process., vol. 59, no. 2, pp. 774–786,Feb. 2011.

[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] H. Wang, L. Lightfoot, and T. Li, "On phy-layer security of cognitive radio: Collaborative sensing under malicious attacks," in Proc. 201044th Annu. Conf. Inform. Sci. and Syst. (CISS), Mar. 2010, pp. 1–6.

[10] 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.

[11] 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.

[12] 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.

[13] W. Zhang, R. Mallik, and K. Ben Letaief, "Cooperative spectrum sensing optimization in cognitive radio networks," in Proc. IEEE Int.Conf. Commun., 2008 (ICC '08), May 2008, pp. 3411–3415.

[14] 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.

[15] 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.

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

[17] X. Luo, M. Dong, and Y. Huang, "On distributed fault-tolerant detection in wireless sensor networks," IEEE Trans. Comput., vol. 55, no. 1, pp. 58–70, Jan. 2006.

[18] C. M. Bishop, Pattern Recognition and Machine Learning (Information Science and Statistics). Secaucus, NJ: Springer-Verlag, 2006.

[19] B. Chen, R. Jiang, T. Kasetkasem, and P. Varshney, "Channel aware decision fusion in wireless sensor networks," IEEE Trans. SignalProcess., vol. 52, no. 12, pp. 3454–3458, Dec. 2004.

[20] S. Boyd and L. Vandenberghe, Convex Optimization, 1st ed. New York: Cambridge Univ. Press, 2004.

[21] Q. Zhang, P. Varshney, and R. Wesel, "Optimal bi-level quantization of i.i.d. sensor observations for binary hypothesis testing," IEEE Trans.Inform. Theory, vol. 48, no. 7, pp. 2105–2111, Jul. 2002.

[22] A. R. Webb, Statistical Pattern Recognition, 2nd ed. Chichester, West Sussex, England: Wiley, 2001.

[23] S. M. Kay, Fundamentals of Statistical Signal Processing: Detection Theory, 1st ed. Upper Saddle River, NJ: Prentice-Hall, 1998.

[24] R. Viswanathan and P. Varshney, "Distributed detection with multiple sensors I. Fundamentals," Proc. IEEE, vol. 85, no. 1, pp. 54–63, Jan. 1997.

[25] D. J. Hand, Construction and Assessment of Classification Rules, 1st ed. Chichester, West Sussex, England: Wiley, 1997.

[26] P. Varshney, Distributed Detection and Data Fusion, 1st ed. New York: Springer-Verlag, 1997.

[27] S. M. Kay, Fundamentals of Statistical Signal Processing, Volume I: Estimation Theory, 1st ed. Upper Saddle River, NJ: Prentice-Hall,1993.

[28] P. Rousseeuw and A. Leroy, Robust Regression and Outlier Detection. New York: Wiley, 1987.

[29] A. P. Dempster, N. M. Laird, and D. B. Rubin, "Maximum likelihood from incomplete data via the EM algorithm," J. Royal Statist. Soc., Ser.B, vol. 39, no. 1, pp. 1–38, 1977.