ISSN: 0974-2115
www.jchps.com Journal of Chemical and Pharmaceutical Sciences

Improving Network Performance and Security in WSN using Decentralized Hypothesis Testing

C. Anuradha*, V. Khanna
Department of CSE, Bharath University, Chennai-73
Dean Info, Bharath University, Chennai-73
***Corresponding author:E-Mail: anuradha.ak23@gmail.com**

ABSTRACT

Wireless sensor networks (WSN) due to its wireless dynamic nature and open medium the network is vulnerable to hub bad conduct emerging from altering by an unauthorized user otherwise required to some other component like conjunction down. Its results are software or hardware degradation. In this consider that a fragment of the supervise detector are encompass by an adversary. Hypothesis compromised sensors are captured and reprogrammed to transmit duplicate data in order to confuse the fusion centre. The binary hypothesis testing is used in the fusion centre. In Binary hypothesis testing, honest nodes are transmit their binary decisions and the deviate nodes are transmit fictitious messages. The aim of the fusion centre is to identify the presence of misbehaving nodes and also identify the position of nature. Then the fusion centre estimates the nodes utilize points on the receiver operating characteristic (ROC) curve. The evaluation of the interchange operating point is solved by using the expectation maximization (EM) algorithm. The result of the Expectation Maximization algorithm is used to categorize the nodes and also to find the byzantine node down. The proposed weighted majority algorithm is used to identify the reliable path for the data transmission thereby improving the network performance and security.

KEY WORDS: ROC, EM, Byzantine attack, Binary hypothesis testing, Expectation Maximization.

1. INTRODUCTION

It contains number of sensor nodes, in that the nodes are report the information to a fusion center over wireless links. Detectors have restricted storage, processing and communication potential due to its size and power conditions. Due to environmental effects or hardware de gradation the sensor nodes may fail in a large network. In this situation, few situations a fault node halt its performance and in few other situations sensor nodes are misbehaving and reporting false data to the fusion center.

Furthermore, the wireless transmission medium is makes possible for the aggressor to concentrate data from sensor transmissions because it is more vulnerable to eavesdropping. As a result, the adversary [3] can additionally place its own detector convergence aimed at jamming the honest nodes transmissions or in order to confuse the fusion center transmit false data.

Byzantine Attack: These networks are more danger to influence. The networks are visualized to be speeded over a region, the fraction of detector nodes are compromised by an opponent. Then these compromised nodes are captured and modified by an adversary and also in order to confuse the combination focus opponents place its own nodes to transfer incorrect messages. In this consider the wireless sensor network is designed which undergoes a Byzantine attack in that a fraction of sensor nodes cooperatively transmit fictitious messages in order to impair the capability of the fusion center. Thus in the network, the sensor nodes which is under a visualize control are mention as fault tolerant. This type of attack is named as a byzantine attack

2. METHODS

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 correct nodes transfer their binary decisions and the vulnerable nodes transmit imaginary information to the fusion center. In binary hypothesis testing, the sensor nodes frequently make a neighborhood decision regarding the state of the hypothesis in order to lower their frequencies requirement and energy expenditures and then only send their binary decision to the fusion center. Then the integration center will identify the presence of misbehaving nodes from 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 integration center is to identify the presence of illegal/wrong nodes and also to identify the status.

Receiver Operating Characteristic (ROC) curve: It is used to estimate the operating points of the nodes. In this demonstration that each portion of nodes can be discover 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 decision in that class [1].

Expectation Maximization (EM) Algorithm: This algorithm is used to solve the difficulties of byzantine attack in the existence of misbehaving conjunctions. In the network, estimate the maximum likelihood of the nodes operating points is formulated and then solved using the expectation maximization algorithm.

The result of the expectation maximization algorithm is then used to classify the nodes and to solve the byzantine node problem. Then the results are compared with the reputation based schemes. It shows a significant improvement in both hypothesis testing results and classification of the nodes. Algorithm shown is guaranteed to increase the log-likelihood function for every update. Thus using the expectation maximization algorithm solved the byzantine attack problem thereby improves the security in the wireless sensor networks. Evaluate the performance of the expectation maximization algorithm that show this proposed algorithm significantly outperforms than the reputation based methods in detection of the hypotheses and classification of the nodes. Moreover the proposed algorithm is faster than the reputation based method.

Weighted Majority (WM) Algorithm: The weighted majority algorithm is used to find the reliable path in the network. The reliable path is identified for the information between the nodes. Thus it improves the network performance in the wireless networks.

System model: It is 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 while the byzantine node are transmit the fictitious messages to the fusion center. Then implement the binary hypothesis testing in the combination in order to identify presence of misbehaving nodes in the network. Then estimate the operating points of the nodes on the receiver operating attribute curve. The expectation maximization algorithm is used to categorize the detector and find the byzantine node failure and then using the weighted majority algorithm identifies the reliable path for the data transmissions. There by increase the network execution and protect in the wireless sensor networks.

3. CONCLUSION

In this research work, examine the difficulties of byzantine attack in the existence of number of misbehaving nodes in the result of the binary hypothesis method. It is used to solve the byzantine attack problem arise in the wireless sensor networks. Weighted Majority algorithm is used to identify the reliable path for the message conveyance between the confluences. Thereby improves performance and security in the wireless sensor network**.**

REFERENCES

Abdelhakim M, Lightfoot LE, and Li T, Reliable data fusion in wireless sensor networks under Byzantine attacks, in Proc. Military Commun. Conf., 2011 (MILCOM 2011), 2011, 810–815.

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

Brintha Rajakumari S, Nalini C, An efficient data mining dataset preparation using aggregation in relational database, Indian Journal of Science and Technology, 7, 2014, 44-46.

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

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

Jayalakshmi V, Gunasekar NO, Implementation of discrete PWM control scheme on Dynamic Voltage Restorer for the mitigation of voltage sag /swell, 2013 International Conference on Energy Efficient Technologies for Sustainability, ICEETS, 2013, 1036-1040.

Kaliyamurthie KP, Parameswari D, Udayakumar R, QOS aware privacy preserving location monitoring in wireless sensor network, Indian Journal of Science and Technology, 6 (5), 2013, 4648-4652.

Kaliyamurthie KP, Udayakumar R, Parameswari D, Mugunthan SN, Highly secured online voting system over network, Indian Journal of Science and Technology, 6 (1), 2013, 4831-4836.

Khanaa V, Thooyamani KP, Saravanan T, Simulation of an all optical full adder using optical switch, Indian Journal of Science and Technology, 6 (1), 2013, 4733-4736.

Khanaa V, Thooyamani KP, Using triangular shaped stepped impedance resonators design of compact microstrip quad-band, Middle - East Journal of Scientific Research, 18 (12), 2013, 1842-1844.

Kumaravel A, Dutta P, Application of Pca for context selection for collaborative filtering, Middle - East Journal of Scientific Research, 20 (1), 2014, 88-93.

Penna F, Sun Y, Dolecek L and Cabric D, Detecting and counteracting statistical attacks in cooperative spectrum sensing, IEEE Trans. Signal Process, 60 (4), 2012, 1806–1822.

Raj MS, Saravanan T, Srinivasan V, A modified direct torque control of induction motor using space vector modulation technique, Middle - East Journal of Scientific Research, 20 (11), 2014, 1572-1574.

Rawat A, Anand P, Chen H, and Varshney P, Collaborative spectrum sensing in the presence of Byzantine attacks in cognitive radio networks, IEEE Trans. Signal Process, 59 (2), 2011, 774–786.

Rawat A, Anand P, Chen H, and Varshney P, Countering Byzantine Vulnerabilites, Int.Conf. Acoust. Speech and Signal Process.(ICASSP), Mar. 2010.

Saravanan T, Raj MS, Gopalakrishnan K, VLSI based 1-D ICT processor for image coding, Middle - East Journal of Scientific Research, 20 (11), 2014, 1511-1516.

Sengottuvel P, Satishkumar S, Dinakaran D, Optimization of multiple characteristics of EDM parameters based on desirability approach and fuzzy modeling, Procedia Engineering, 64 (1), 2013, 1069-1078.

Soosahabi R and Naraghi-Pour M, Flexible distributed detection in wireless sensor networks, IEEE Trans. Inf.Forensics Security, 7 (4), 2012, 1118–1126.

Sundararajan M, Optical instrument for correlative analysis of human ECG and breathing signal, International Journal of Biomedical Engineering and Technology, 6(4), 2011, 350-362.

Thamotharan C, Prabhakar S, Vanangamudi S, Anbazhagan R, Anti-lock braking system in two wheelers, Middle - East Journal of Scientific Research, 20 (12), 2014, 2274-2278.

Udayakumar R, Khanaa V, Saravanan T, Saritha G, Retinal image analysis using curvelet transform and multistructure elements morphology by reconstruction, Middle - East Journal of Scientific Research, 16 (12), 2013, 1781-1785.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and fabrication of dual clutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1816-1818.

Vanangamudi S, Prabhakar S, Thamotharan C, Anbazhagan R, Design and calculation with fabrication of an aero hydraulwicclutch, Middle - East Journal of Scientific Research, 20 (12), 2014, 1796-1798.

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