Asian Journal of Information Technology 15 (14): 2322-2327, 2016
ISSN: 1682-3915

Jammer Localizatoin in Wireless Sensor Network Using Percolation and Poisson Process

[1]A. Mummoorthy and [2]S. Suresh Kumar
[1]K.S.R. College of Engineering,
[2]Vivekanandha College of Technology for Women, Tiruchengode,
Namakkal District, Tamil Nadu, India

Abstract: The security risk in wireless sensor network had appeared in the recent days. Ensuring of wireless communication dependability was especially harmful because of the jamming attacks. Inorder to exploit a wide range of defense strategies in wireless network the position of the jammer must be found out. By identifying the jammer position the defender could actively able to eliminate the attacks. Thus in this study, the localization was used to obtain a high accuracy. The result shows that the minimizing of error based framework achieved a better performance compared to the existing schemes.

Key words: Security risk, defender, localization, attacks, India

INTRODUCTION

The main critical attributes in any communication network could be the security whether it was wired or wireless networks. Also, wireless networks can be easy to be build, since the technology was advanced at the present time. WMANs and WLANs were the main reality so access the internet inorder to access any information. But the security flaw would be accomplished easily in wireless then the wired network as it was undoubtedly easy to access. The communication between any two wireless capable nodes could be feasible to block using various malicious techniques. By designing the network security architectures the wireless security threads could be addressed (Yang and Chen, 2009; Bahl and Padmanabhan, 2000; Wenyuan *et al*., 2005). However in PHY and MAC layers, the jamming techniques such as brute force attack could be detected easily. Inorder to evade detection of vulnerabilities in higher layers the jammers were accomplished as one of the intelligent ways. There were many commercial jamming devices available to attack the wireless networks. With a little effort the jamming attacks could be launched. The reasons were the communication of wireless medium was shared by nature and another was that most wireless networks devices could be easily purchased and reprogrammed inorder to interfere with communication among the nodes. For example, any device any be programmed to prevent users to send or receive messages which disrupts the network communications (Liu *et al*., 2011a). The physical properties such as power, etc., were dictated the extent of jamming. The unwanted and disruptive which was similar to create the denial-of-service was the jamming which was no different than the normal radio propagation. The efficiency criterion that enumerates the jamming were the energy efficiency, probability of detection, level of DoS and strength against physical layer techniques. Also, the ideal jamming attack would be similar to the one which satisfies these criteria. The metrics which were used to capture the jammer's behavior was described by (Pelechrinis *et al*., 2011; Sundar and Mahesh, 2015; Cheng *et al*., 2012).

The activation of devices accidently such as microwave ovens which does not serve a malicious cause was one of the effects of jamming occurrence. The legality of jammers to operate was based on some specific laws of the area. The algorithm mainly used the localization mainly depend upon the Packet Delivery Ratio (PDR) (Konstantinos *et al*., 2009; Liu *et al*., 2011b). The various application scenarios were:

- Military or security applications
- Civilian applications, etc. (Liu *et al*., 2009)

EFFECTIVENESS AND ATTACK MODELS OF JAMMING

The technology of jamming does not generally discriminate between the desirable communication and undesirable. A device which was used to block all radio communication which operates on radio frequencies to a limited range were called the jammers.

Corresponding Author: A. Mummoorthy, K.S.R. College of Engineering, Tiruchengode, Namakkal District, Tamil Nadu, India

Effectiveness: The jammers effectiveness could be measured using the metrics such as:

- Packet Send Ratio (PSR)
- Packet Delivery Ratio (PDR)

In order to fill a wireless channel there was an assumption that jammer continuously emits RF signals and because of that the legitimate traffic would be completely blocked. But, a jammer could start interference as soon as it detects the transmission of messages from sender or receiver until then the jammer could remain silent. So a jammer could interfere with the physical transmission and the reception of wireless communications. The interference of legitimate transmission of wireless communication was the objective of jammer. So, the goal of the jammer could be achieved by either preventing the source from sending a message or reception of legitimate packets. Consider X and Y were two legitimate wireless participants and Z denotes the jammer (Chimankar and Nandedkar, 2015; Dineshbabu and Thirunavukarasu, 2014;Padmapriya and Senthil, 2014). The PSR could be measured as follows. If X intends to send m messages, but he received only n messages then PSR is:

$$PSR = \frac{n}{m} \quad (1)$$

$$PDR = S_{p_{send-data}} / S_{q_{receive-data}} / S_{p_{receive-ack}} \quad (2)$$

That is PDR could be calculated either if the data was send from the sender X but the receiver Y could not able to decode it $(S_{p_{send-data}})$ or if the receiver Y could calculate the number of packets that passed the CRC check which preambles received $(S_{q_{receive-data}})$ or the receiver Y send an acknowledgement signal to the sender X $(S_{p_{receive-ack}})$. But, PDR can be assigned zero (0) when the packets were received. Some other techniques were signal strength, carrier sensing time, sending range and hearing range (Liu *et al*., 2010; Jayasree and Sabeena, 2015; Priya *et al*., 2015).

Attack models: There are totally four jammer attacking models (Jaipriya, 2015; Kadam and Patil, 2014):

- Constant jammer
- Deceptive jammer
- Random jammer
- Reactive jammer

The jammers which emit a radio signal and randomly transmit the arranged bits to the channel were called as constant jammer. The constant jammer does not wait for the channel to become idle and it does not follow any MAC layer protocol. The deceptive jammer injects the regular packets continuously to the channel and the packets get deceived by the usual nodes and the normal nodes checks the prelude and remain noiseless. The random jammers alternate between the period of continuous jamming and inactivity. After a unit of time this jammer stops emitting the radio signal and enters into the sleep mode. Then, after sleeping for another unit of time it wakes up and resumes the jamming. In the reactive jammer model, the jammer will stay quite when the channel is idle. It will transmit the signal as soon as it senses the activity of the channel. The applications of jammer attack models were explained in (Misra *et al*., 2010).

EXISTING METHODS

The gradient decent search and Packet Delivery Rate (PDR) were used to measure the localization of jammers (Sneha and Munmun, 2015). But, the performance evaluation of the search was not discussed. The localization algorithms were iterative- based and the neighbor node changes were caused in one direction. LSQ-based jammer localization algorithm exploits the changes of communication range (Liu *et al*., 2012a). This algorithm achieved lower computational cost, higher localization accuracy and could effectively estimate the location of jammers.

For mapping the extent of the jammed region a protocol was evaluated and the protocol was evaluated using the simulation which shown the various size of jammed region and failure rates. This mapping protocol shows quickly the single dominant group of jammed nodes when the wireless networks were moderately connected (Wood *et al*., 2003). A multipath routing protocol was proposed which was capable to search multiple node-disjoint paths. The traffic rate was optimized using the load balancing algorithm. The result shows that they have achieved higher energy efficiency, energy aware routing and directed transmission (Lu and Wong, 2007).

NETWORK MODELING (PROPOSED SYSTEM)

Let us assume, the wireless sensor network consists of N sensor nodes and each having a base station and the transmission range for all the nodes were same. For the larger network with many number of base station consider they were separated into small ones inorder to assume our network model. By considering the percolation model

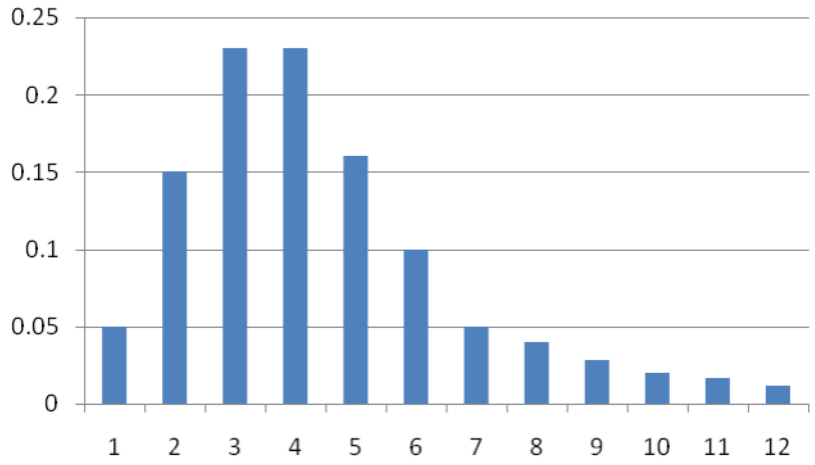

Fig. 1: Poisson model with $\mu = 3$

(Huang *et al*., 2011) the phase transition in the performance of network would be from a disconnected state to a connected state. In this study, the average of number of nodes per unit area will be considered as μ. Then, the proposition was proposition 1: In a Poisson Boolean model with radius r, the probability that there are m nodes in an area A was given by:

$$p(N_A = m) = e^{-\mu A}\frac{(\mu A)^m}{m!} \tag{3}$$

Consider if two nodes were connected and the distance between them is no longer the maximum range r. The sets of nodes V and edges E constitute a graph G (V, E) and any node pair j, k was connected then the Euclidean distance between them would be less than or equal to the transmission range. Figure 1 shows the Poisson model with $\mu = 3$.

With the same transmission range the neighbor nodes within those ranges can be able to receive the message. The entire sensor nodes based on the jamming status they were confidential into four types:

- Trigger node
- Victim node
- Boundary node
- Unaffected node

In proposition 2; the network connectivity could be parameterized using the percolation probability $\theta(\mu)$ which could be defined as the probability that $|C_1(0)|$ where $C_1(0)$ was the cluster to where the origin was connected. Then, the critical intensity (μ_c) based on the theory of continuum percolation would be given as:

$$\theta(\mu)\begin{cases} = 0 \text{ if} \mu < \mu_c \\ > 0 \text{ if} \mu > \mu_c \end{cases} \tag{4}$$

and the cluster probability would be stated as:

$$p(\exists C_1 : |C_1| = \infty)\begin{cases} = 0 \text{ if} \mu < \mu_c \\ = 1 \text{ if} \mu > \mu_c \end{cases} \tag{5}$$

the network would behave like two regimes. They were:

- Sub-critical regime ($\mu<\mu_c$)
- Super-critical regime ($\mu>\mu_c$)

There exists no infinite cluster of nodes when $\mu = \mu_c$ in 2-D space. Under the following condition with d as the dimension of space, the percolation behavior would be invariant:

$$(\theta, r) \leftrightarrow (s^{-d}\theta, sr) \tag{6}$$

The load balancing ratio (φ) to evaluate the load balancing level over the different multipath was given as:

$$\varphi(r') = \frac{\left(\Sigma_{j=1}^{N} r_j p_j\right)^2}{N\Sigma_{j=1}^{N}\left(r_j p_j\right)^2} \tag{7}$$

The traffic rates allocated to all the routes were denoted as r'. When, the traffic was perfectly balanced the load balance ratio was obtain the global maximum of 1. The average energy dissipated was measured using the node energy consumption which would lead to transmit a data packet from source to the receiver. The

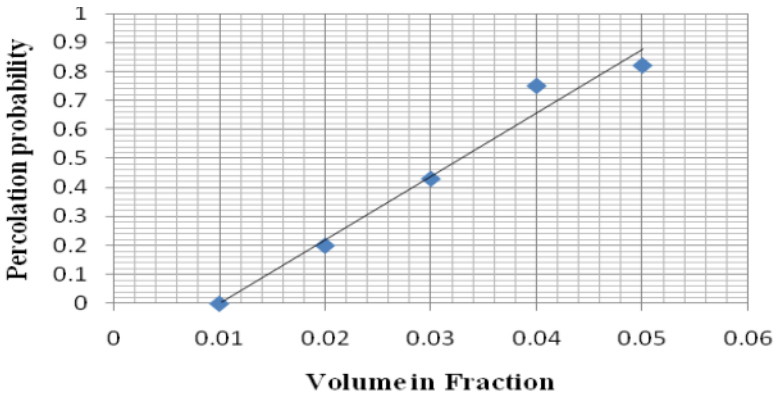

Fig. 2: Percolation probability as distribution

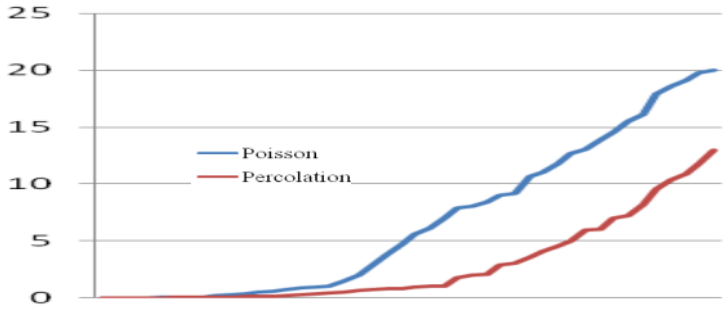

Fig. 3: Simulation result

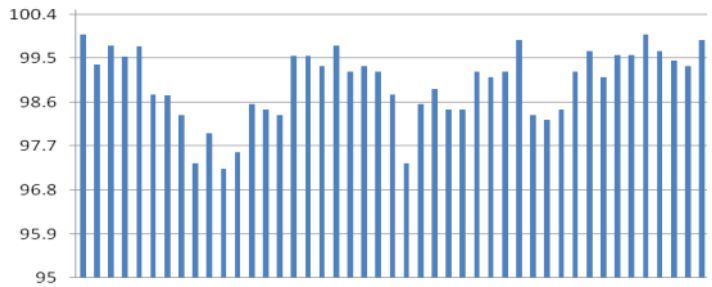

Fig. 4: Energy utilization

ratio of successfully percolated structures to the number of simulation performed was used to calculate the percolation probability (Fig. 2). The simulation result for comparing the poisson model and the percolation probability was shown in Fig. 3. The energy efficiency level of the wireless network could also be calculated from the node energy consumption equation:

$$Con = \frac{\Sigma_{i=1}^{L}\left(\theta_{i,init} - \theta_{i,rest}\right)}{L\Sigma_{j=1}^{T} data\, C_j} \quad (8)$$

Where:

L = The number of nodes

$\theta_{i, init}$ and $\theta_{i, rest}$ = The initial and residual energy levels of node I

T = The number of receiver nodes

data C_j = The number of data packets

We could able to observe that the energy consumption was lower and the direct transmission improves the energy efficiency (Liu *et al*., 2012b; Kumar and Krishna, 2013). The energy utilization of nodes during the message conversation is shown in Fig. 4.

CONCLUSION

The performance of wireless sensor networks would be affected by the jammers which has caused because of

the wireless broadcast nature. In this study, a framework was deigned to localize the jammers and the energy efficiency was improved. The localization was combined with the clusters of nodes and in particular the percolation theory explained the phase transition of the targeted network. By approaching the jamming problems in wireless sensor networks, we believe that the network perspective could be able to widen the research and could be able to bring out some interesting results. The identification of one jammer would enable the transfer of data among the various nodes and provides more security mechanism.

REFERENCES

Bahl, P. and V.N. Padmanabhan, 2000. RADAR: An in-building RF-based user location and tracking system. Proceedings of the 19th Annual Joint Conference of the IEEE Computer and Communications Societies, March 26-30, 2000, Tel Aviv, Israel, pp: 775-784.

Cheng, T., P. Li and S. Zhu, 2012. An algorithm for jammer localization in wireless sensor networks. Proceedings of the 2012 IEEE 26th International Conference on Advanced Information Networking and Applications, March 26-29, 2012, IEEE, Fukuoka, Japan, ISBN: 978-1-4673-0714-7, pp: 724-731.

Chimankar, A.S. and V.S. Nandedkar, 2015. Effective approach for localizing jammers in wireless sensor network. Int. J. Sci. Res., 4: 914-918.

Dineshbabu, B. and T. Thirunavukarasu, 2014. Survey on localization of the sensor nodes in wireless sensor networks. Int. J. Comput. Sci. Trends Technol., 2: 49-51.

Huang, H., N. Ahmed and P. Karthik, 2011. On a new type of denial of service attack in wireless networks: The distributed jammer network. IEEE. Trans. Wirel. Commun., 10: 2316-2324.

Jaipriya, S., 2015. A framework for detection of jammers in wireless sensor network. Int. J. Innov. Res. Comput. Commun. Eng., 3: 1653-1660.

Jayasree, M. and J. Sabeena, 2015. Impact of jammers and the localization methods in wireless networks. Int. j. Comput. Sci. Math. Eng., 2: 72-76.

Kadam, M.S.S. and Y.M. Patil, 2014. Detection and localization of wireless jammer. Int. J. Recent Innov. Trends Comput. Commun., 2: 4172-4175.

Kumar, P.K. and P.P.M. Krishna, 2013. Detecting and detaching reactive jammers in wireless sensor network. Int. J. recent. Technol. Eng., 2: 89-91.

Liu, H., X. Wenyuan, Y. Chen and Z. Liu, 2009. Localizing jammers in wireless networks. Proceedings of the 2009 IEEE International Conference on Pervasive Computing and Communications PerCom, March 9-13, 2009, IEEE, Galveston, Texas, ISBN: 978-1-4244-3304-9, pp: 1-6.

Liu, Z., H. Liu, W. Xu and Y. Chen, 2010. Wireless Jamming Localization by Exploiting Nodes Hearing Ranges. In: Distributed Computing in Sensor Systems. Rajaraman, R., T. Moscibroda, A. Dunkels and A. Scaglione (Eds.). Springer Berlin Heidelberg, Heidelberg, Germany, ISBN: 978-3-642-13650-4, pp: 348-361.

Liu, H., Z. Liu, Y. Chen and W. Xu, 2011a. Determining the position of a jammer using a virtual-force iterative approach. Wirel. Netw., 17: 531-547.

Liu, H., Z. Liu, Y. Chen and W. Xu, 2011b. Localizing multiple jamming attackers in wireless networks. Proceedings of the 2011 31st International Conference on Distributed Computing Systems (ICDCS), June 20-24, 2011, IEEE, Minneapolis, Minnesota, ISBN: 978-1-61284-384-1, pp: 517-528.

Liu, Z., H. Liu, W. Xu and Y. Chen, 2012a. Error minimizing jammer localization through smart estimation of ambient noise. Proceedings of the 2012 IEEE 9th International Conference on Mobile Ad-Hoc and Sensor Systems (MASS 2012), October 8-11, 2012, IEEE, Las Vegas, Nevada, ISBN: 978-1-4673-2433-5, pp: 308-316.

Liu, Z., H. Liu, W. Xu and Y. Chen, 2012b. Exploiting jamming-caused neighbor changes for jammer localization. IEEE. Trans. Parallel Distrib. Syst., 23: 547-555.

Lu, Y.M. and V.W.S. Wong, 2007. An energy-efficient multipath routing protocol for wireless sensor networks. Int. J. Commun. Syst., 20: 747-766.

Misra, S., R. Singh and S.V. Mohan, 2010. Information warfare-worthy jamming attack detection mechanism for wireless sensor networks using a fuzzy inference system. Sensors, 10: 3444-3479.

Padmapriya, P.S. and M. Senthil, 2014. Enhancement of an error minimizing framework for localizing jammers in wireless networks: A survey. Int. J. Eng. Technol., 5: 5088-5097.

Pelechrinis, K., I. Koutsopoulos, I. Broustis and S.V. Krishnamurthy, 2009. Lightweight jammer localization in wireless networks: System design and implementation. Proceedings of the 2009 IEEE Conference on Global Telecommunications GLOBECOM, November 30-4, 2009, IEEE, Honolulu, Hawaii, ISBN: 978-1-4244-4148-8, pp: 1-6.

Pelechrinis, K., M. Iliofotou and S.V. Krishnamurthy, 2011. Denial of service attacks in wireless networks: The case of jammers. IEEE. Commun. Surv. Tutorials, 13: 245-257.

Priya, P., S. Udhayakumar and Premkumar, 2015. A novel framework for mobile jammer localization in wireless sensor networks. Int. J. Eng. Res., 3: 366-373.

Sneha, V.T. and P.B. Munmun, 2015. Multiple jammer localization for minimizing error in wireless sensor networks. Int. J. Innov. Res. Comput. Commun. Eng., 3: 8316-8324.

Sundar, R. and C. Mahesh, 2015. Novel approach for localization jammers in wireless network. Int. J. Eng. Comput. Sci., 4: 11547-11552.

Wenyuan, X., W. Trappe, Y. Zhang and T. Wood, 2005. The feasibility of launching and detecting jamming attacks in wireless networks. Proceedings of the 6th ACM International Symposium on Mobile ad hoc Networking and Computing, May 25-27, 2005, ACM New York, USA., pp: 46-57.

Wood, A.D., J.A. Stankovic and S.H. Son, 2003. JAM: A jammed-area mapping service for sensor networks. Proceedings of the 24th 2003 IEEE Symposium on Real-Time Systems RTSS, December 3-5, 2003, IEEE, Charlottesville, Virginia, USA., ISBN: 0-7695-2044-8, pp: 286-297.

Yang, J. and Y.Y. Chen, 2009. Indoor localization using improved RSS-based lateration methods. Proceedings of the IEEE Global Telecommunications Conference, November 30-December 4, 2009, Honolulu, USA., pp: 1-6.