Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

A Novel Technique for Jamming Attack Detection in Wireless Adhoc Networks Using BLMSPC Protocol

S. Pushpa Latha[1], Dr.R. Sabitha[2], Dr.K. Anitha[3], Dr.M. Nalini[4]

[1]Assistant Professor, Jeppiaar Engineering College, Chennai, Tamil Nadu, India. E-mail: latha.spl2004@gmail.com

[2]Professor, Department of CSE, Saveetha School of Engineering, SIMTAS, Chennai, Tamil Nadu, India. E-mail: sabithar.sse@saveetha.com

[3]Associate Professor, Saveetha School of Engineering, SIMTAS, Chennai, Tamil Nadu, India. E-mail: anithak.sse@saveetha.com

[4]Assistant Professor, Saveetha School of Engineering, SIMTAS, Chennai, Tamil Nadu, India. E-mail: nalinim.sse@saveetha.com

ABSTRACT

The wireless ad-hoc networks have become Vulnerable to attacks jamming because of Open Physical Media Shares. Jamming attack is defined as radio signal emission that aims to disturb the transceiver operation. This paper aims to spot jamming attacks, using a proposed protocol is Base line local monitoring with Statistical Process Control (BLMSPC). Local Monitoring is a technique that is used to find the behavior of its neighbors. To find the packet drop ratio (PDR) using statical Process control approach. PDR is defined to the number of packets that have been dropped to the total packets sent. Based upon the packet drop ratio the jamming attack will be detected. The proposed algorithm BLMSPC can be implemented by using network simulator 2. BLMSPC can detect the jamming attack very efficiently and it will increase the overall network performance.

KEYWORDS

Jamming, Constant, Deceptive, Reactive, Baseline Monitoring.

Introduction

Jamming Attack [18] centers on working against a sender or beneficiary that transmits or gets packets. It can transmit uninterrupted signals to the channel so the sender earns busy status, or it can relay daily data packets and continuously force the beneficiary to accept garbage packets. Here, the senders send the packet lucratively to the beneficiary however the jammer sends the radio to disrupt the receiver's message. The diagram below shows the jamming attack.

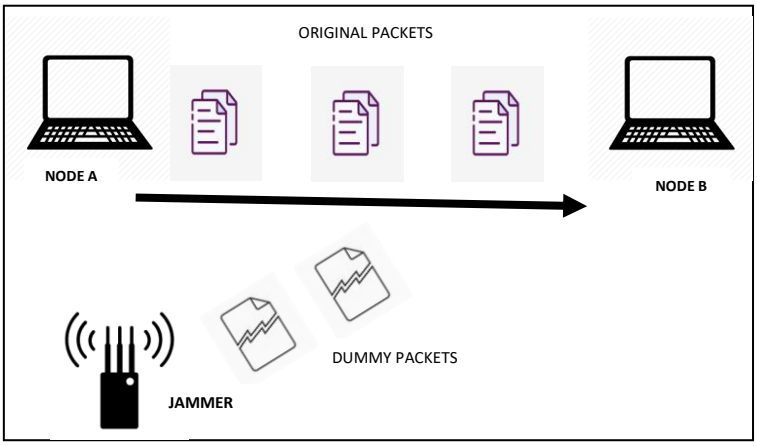


Fig. 1. Jamming Attack scenario

In fig 1 illustrates the jamming attack. Jamming involuntarily interferes with the wireless communication organized as interruption, vibration or collision/crash on the receiver side. It overwhelms the transmitted signals by implementing a massive noise level that reduces the signal-to - noise ratio, thus dropping the likelihood of lucrative packet reception. An optimal jamming attack [5] is intended to have a high energy efficiency, decreased detection

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

potential, unaffected to anti-jamming techniques and also interrupt communications to the full practicable extend [5]. Attacks may be classified as active or passive attacks. Passive attackers allow no submission of messages; they only listen to the medium and snatch Packets which contain IP addresses, node location, etc. They never interrupt contact neither do any physical harm over network, yet request information and breach the security of the network. An instance of this is eavesdropping. Eavesdropper's fundamental reason for existing is to tune in to the transmission and to gain some private data that ought to be left well enough alone during contact. Secret data incorporates passwords for the area, open key, private key or even node [20]. Active attackers disassemble the general activity of a particular hub then aim to operate the entire network. Active attackers are uploading packets to incorrect destinations, falling packets, removing packets, and altering packet content that violates the availability, validity, security, and non-repudiation model [19].

Jamming attack usually defined as four types. Such as Constant, Deceptive, Reactive and random jammer [5], [21],[22].

Constant Jammer

It is consistently transmits irregular unimportant noise signals to the wireless media, and doesn't hold up until the channel is inactive until it is transmitted [26].

Deceptive Jammer

This jammers spray standard packets of noise signals without space among them, continuously [5],[3]; The primary distinguishing feature is that the constant jammer continually discharges random noise signals while the deceptive jammer ceaselessly discharges commotion signals on the medium immediately. The customer then assumes that a legal communication is taking place. Deceptive jamming is easier to spot than persistent jammering. Constant and manipulative jamming hinders communication and goal delivery on the receiver side.

Random Jammer

A spontaneous jammer can sends a noise signal randomly to the wireless medium and contemplatively saves power. This jammer acts as a persistent jammer or a deceptive jammer during a random period, and remains suitable for a second random time. This jammer's having the greatest advantage is, it will absorbs energy.

Reactive Jammer

A reactive jammer that targets packet reception and heavy handedly jams only when the contact channel is occupied [12]-[17]. This jammer remains silent until the channel is tracked, the channel is continuously monitored, and when the packet transmission is detected, it instantly transmits the radio signal. Also these jammers contribute extra time on feeling the channel and spent less time on interrupting the packet. This is also a great call to jamming. The throughput obtained from reactive jammer is always higher compared to other jammers.

Related Work

We now discuss about the jamming attacks detection with various methods.

Nadem Sufyan et.al (2013) has a multi-model method for jamming attacks, identifying the three variables: packet distribution ratio, signal intensity variations and pulse width of the received signal. The jammed region is separated by the multi model. It was launched by using real test bed alternatively for using simulator. The disadvantage of this method is that it can be only used in single transmitter and receiver [6].

Tague et.al (2009) proposed an idea so that the control channel slots will be hidden called the cryptographic key-based mechanism [7]. With some probability only a subset of nodes can be discovered. The function of the characters of compromised nodes allows a distinguished degeneration in the control channel [8]. Also, for identifying the set of jammed control channels they found an algorithm called GUIDE.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

Liu et.al (2010) proposed the RD-DSSS. It is based on using only PN codes to allow the resistance to jamming. For RD-DSSS, the encoding of "0" bit represent two arbitrarily chosen low-correlation PN codes and encoding of "1" bit represent two PN codes always with maximum correlation. At the end of each message the preferred PN codes are attached; hence they decrease their efficiency to communicate with original DSSS. The selected PN codes can be recovered once the transmitted message is received [9].

Liu, Qiang et.al (2013) proposed the idea to defect reactive jamming based on adaptive immune system called an immunological anti-jamming method. It consists of three module functions. The monitoring agent tests the neighbors' actions and it will transfer the outcome to the decision agent. The decision agent identifies the jamming attacks based upon the known jamming attacks. The database of jamming gets upgraded when they are recognized by the abnormal behavior of the jammers. Lastly, recovery agents eliminates jamming attacks on various mechanism like frequency hopping spread spectrum and path switching, direct sequence [10].

L. Lazos et.al (2012) proposed the Randomized Distributed using frequency hopping. It prevents from control jamming and as identifies nodes using its unique sequence and that does not include them from the network. It has the advantage where the node works under a unique hopping sequence. The method is not applicable for full duplex communication [11]. It has no extra overhead. The method is used to find a temporary solution for re-establishment of control channels.

Model Assumptions and Metrices

Network Model

A Multichannel Multi-radio wireless Ad hoc network is taken into consideration. K orthogonal frequency bands are the network in which static method approach is operated. Primary ratio (PR) activity is the factor by which K (t) varies in case of dynamic methods. The variable K represents average number of idle channel [23].The capacity of Multichannel wireless networks having two settings. (1) Arbitrary networks (2) Random Networks. Based upon the random networks we choose the node locations are randomly. This method is more precisely independently and evenly chosen on the network [5]. A recent study [2] shows in a network circumstances the total number of nodes N will be placed randomly in the Ad hoc networks. One or more ratios are used to refer to each node. The source node S can send the data to the destination node D for every session may traverse through the multiple nodes in the network. We assume that there is a total of M orthogonal channels in the wireless network, denoted by CH= {ch_1, ch2,..ch_m} and there is no inter channel interference. The number of working channels allocated to node i is denoted as CH_i. In between any two nodes the transmission nodes are present in network.

(i) Direct Transmission
(ii) Cooperative Transmission

[1] The direct transmission is, node x can directly transmit the data to the neighboring node y Over one link. The cooperative transmission is, three links are involved in x and z. (x->z),(x->y) and (y->z). Here the node y acts as an intermediate or cooperative relay for transmission between the node x and the node z.
[2] The attainable rate among the source and destination node is indicated for the direct transmission mode as Where

DT - Direct Transmission
s - Source node
d - Destination node
W - Available bandwidth of channels

Adversarial Model

Irreparable corruption occurs to any message received by a node which is usually between jamming range and the jammed frequency. If jamming attacks are inside the distance of Rmax then it will adjust for the network nodes of the

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

jammed frequency band being defined for detection [2].

Proposed Algorithm for Detecting Jamming Attack

BLMSPC is the convention in which jamming attack efficiency id detected. BLMSPC has three methods to cover local tracking at baseline [25][27].

1. Local Monitoring is done by BLM, in wireless Ad Hoc network; a group of nodes we can call as guard nodes. The guard nodes can perform their own task as well as it will be doing the monitoring function. Monitoring means it will observe the neighboring node for how many packets will forwarded to the next node without dropping any packets within the time period (T) [25].
2. Guard node maintains the jamming pattern database table. The guard node calculates the packet drop ratio (PDR) by using the statistical process control method. If the PDR is greater than the threshold values then there is a jamming attack.
3. A higher value of PDR indicates that the node is attacking node. Guard nodes send the message to all nodes to change the channel of transmission. Whenever there is update in jamming pattern database, new jamming attack is discovered. After that guard node share this database table with neighbors at every time slot.

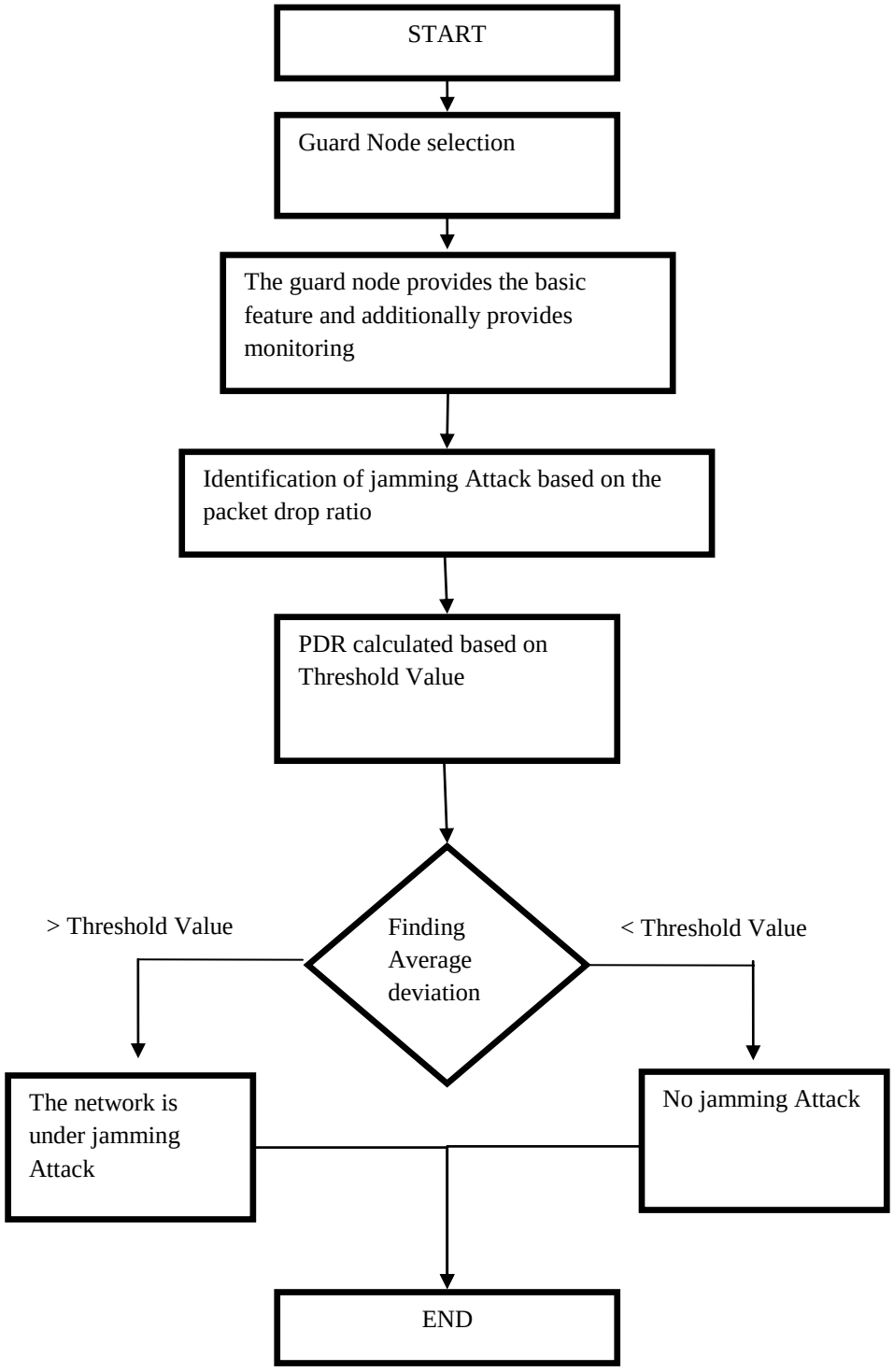
The proposed BLMSPC jamming detection algorithms are discussed in Figure 2.

Procedure for jam(P_k, PDR_{thresh})
Input: Total number of packets(n),current PDR
Output: Average of the packet drop ratio( )
For(i=1 to P_k)
Begin
For(j=1 to n)
Begin
If(current PDR_j==0)
Then
Assign no jamming attack
end if
If (current PDR_j > PDR_{thresh})
//There is a jamming attack.
If ((0<current PDR_j)&&(current PDR_j < = PDR_{thresh})) then
There is a jamming attack and declare true
//Guard node send the message to all nodes to change the channel of transmission.
// Jamming pattern database updated when a new jamming attack was detected.
//Guard node share this database table with neighbors at every time slot
//return PDR_j
//All nodes continue to update the current PDR to their database
Else
There is no jamming attack and declare false
end if

Fig. 2. Proposed jamming Attack Detection Algorithm

The below diagram represent the sequence of process of proposed method.

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.



Simulation Results

Simulation outcome study of the Network Structure, Jammer Detection, using the proposed method BLMSPC. The parameters of simulation can be described below.

Table 1. Simulation parameters

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

Simulation parameters	Values
Number of nodes	50
Packet size	512
Size of packet header	25 bytes
Topology Range	896,837
Simulation time	20
Antenna	unidirectional Antenna
Application	FTP
Routing	AODV
Buffer size	50 packets

1) Network Formation

The figure 3 below represents the process of network formation. Network Formation is a group of nodes in this module that processes unique identification features for each node (which is like n1, n2, n3,..nn)

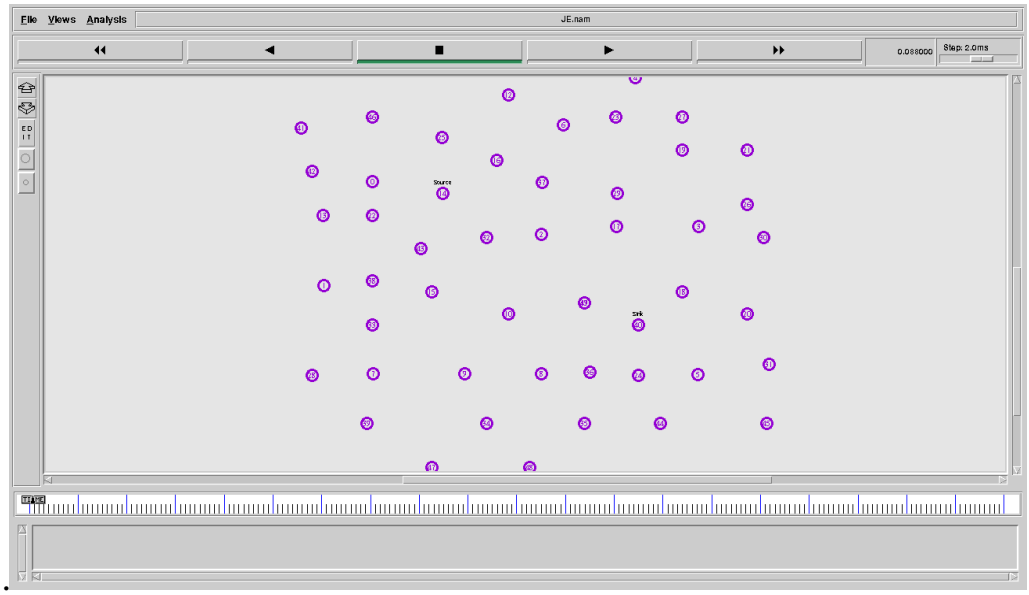


Fig. 3. Network formation

Reactive Jammer

Reactive jammer pays attention to any interference on the channel in fig 4 reveals; also, in these circumstances it conveys a signal instantaneously to collapse with the current signal on the channel remains. Unfortunately, it is also low on energy [5].

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

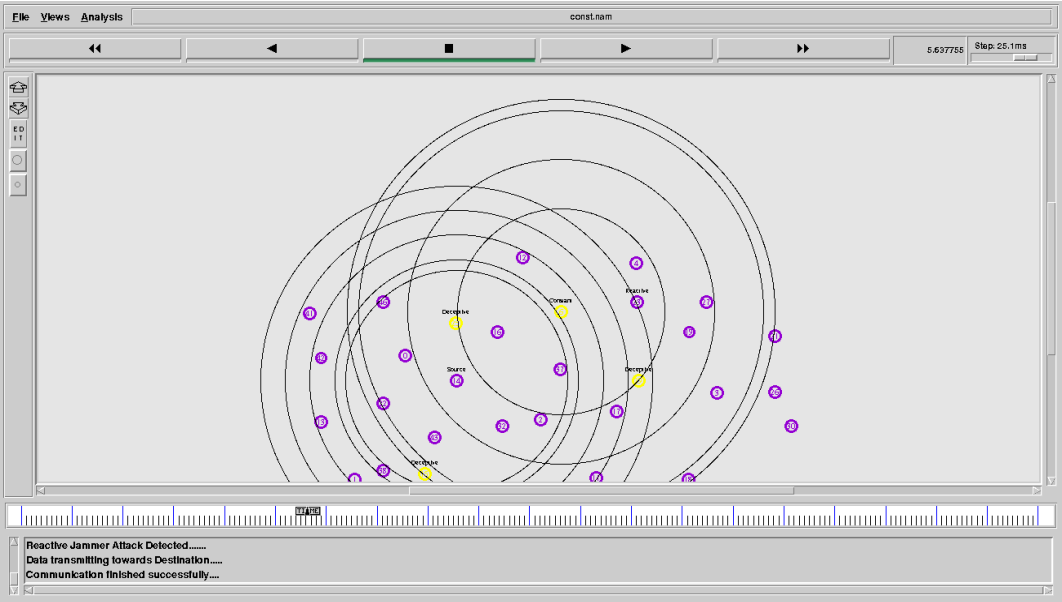


Fig. 4. Reactive Jammer

1. Performance Metrics

Impact of network load for various values on the overall network throughput is looked over in this field.
PDR and throughput are the performance metrics assumed for estimation of jamming attack. It is assumed that A is an attacker node. The probability for one attacker node present in the network is identified

$$P(A) = 1\text{-}P(\hat{A}) \quad (1)$$

If the probability for no attacking node is found in the network, then the probability is in Equation.

$$P(A) = P(A) / P(S) \quad (2)$$

i) Packet Delivery Ratio

The packet delivery ratio is the ratio of the packets received successfully to the complete packets sent [24].

$$\text{Packet Delivery Ratio} = \frac{\sum No.\ of\ packets\ received}{\sum No.Of\ packets\ sent} * 100 \quad (3)$$

ii) End to End Delivery (EED)

The average amount of the delay distinction of each and every data packet received by the sink node and the time the data packet is sent by the source nodes is defined by another network activity monitor called End to End Delay. (Muhammad Farhan Khan et.al 2013.)

$$EED = \sum_{i=1}^{P_{Received}} (T_{Received} - T_{Ranmissioni}) / P_{Received}$$

$T_{Received}$ Represents the duration of when the sink node receives the data packet
$T_{Ranmissioni}$ Represents the time when each source node produces the data packets

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

Conclusion

This research work proposes a novel technique to recognize jamming attack utilizing the protocol called BLMSPC that effectively mitigates the jamming attack. BLMSPC focuses on neighboring observation. Furthermore, the statistical process control (SPC) is implemented to find the packet drop ratio (PDR) within the local monitoring node of the baseline. We also showed the PDR and End to End Delay in performance matrices'. Through extensive simulation using NS2 we show that the proposed algorithm can effectively detect the jamming attack and maintain overall network performance.

References

[1] Cheng, Y., Li, H., Shila, D.M., & Cao, X. (2014). A systematic study of maximal scheduling algorithms in multiradio multichannel wireless networks. *IEEE/ACM Transactions on Networking*, *23*(4), 1342-1355.

[2] Alicherry, M., Bhatia, R., & Li, L. (2005). Joint channel assignment and routing for throughput optimization in multi-radio wireless mesh networks. *In Proceedings of the 11th annual international conference on Mobile computing and networking*, 58-72.

[3] Wunder, G., & Zhou, C. (2009). Queueing analysis for the OFDMA downlink: Throughput regions, delay and exponential backlog bounds. *IEEE Transactions on Wireless Communications*, *8*(2), 871-881.

[4] Shi, Y., & Hou, Y.T. (2008). A distributed optimization algorithm for multi-hop cognitive radio networks. *In Proc. IEEE INFOCOM*, 1512–1520.

[5] Ratna, S.R., & Ravi, R. (2015). Survey on jamming wireless networks: Attacks and prevention strategies. *International Journal of Computer and Information Engineering*, *9*(2), 642-648.

[6] Sufyan, N., Saqib, N.A., & Zia, M. (2013). Detection of jamming attacks in 802.11 b wireless networks. *EURASIP Journal on Wireless Communications and Networking*, *2013*(1), 1-18.

[7] Tague, P., Li, M., & Poovendran, R. (2009). Mitigation of control channel jamming under node capture attacks. *IEEE Transactions on Mobile Computing*, *8*(9), 1221-1234.

[8] Chan, A., Liu, X., Noubir, G., & Thapa, B. (2007). Broadcast control channel jamming: Resilience and identification of traitors. *In IEEE International Symposium on Information Theory*, 2496-2500.

[9] Liu, Y., Ning, P., Dai, H., & Liu, A. (2010). Randomized differential DSSS: Jamming-resistant wireless broadcast communication. *In Proceedings IEEE INFOCOM*, 1-9.

[10] Liu, Q., Yin, J., & Yu, S. (2013). A bio-inspired jamming detection and restoration for WMNs: in view of adaptive immunology. *In International Symposium on Cyberspace Safety and Security*, *Springer*, *Cham*, 243-257.

[11] Liu, S., Lazos, L., & Krunz, M. (2011). Thwarting control-channel jamming attacks from inside jammers. *IEEE Transactions on mobile computing*, *11*(9), 1545-1558.

[12] Wang, L., & Wyglinski, A.M. (2011). A combined approach for distinguishing different types of jamming attacks against wireless networks. *In Proceedings of 2011 IEEE Pacific Rim Conference on Communications, Computers and Signal Processing*, 809-814.

[13] Richa, A., Scheideler, C., Schmid, S., & Zhang, J. (2012). An efficient and fair MAC protocol robust to reactive interference. *IEEE/ACM Transactions on Networking*, *21*(3), 760-771.

[14] Strasser, M., Danev, B., & Čapkun, S. (2010). Detection of reactive jamming in sensor networks. *ACM Transactions on Sensor Networks (TOSN)*, *7*(2), 1-29.

[15] Awerbuch, B., Richa, A., & Scheideler, C. (2008). A jamming-resistant MAC protocol for single-hop wireless networks. *In Proceedings of the twenty-seventh ACM symposium on Principles of distributed computing*, 45-54.

[16] Xuan, Y., Shen, Y., Nguyen, N.P., & Thai, M.T. (2011). A trigger identification service for defending

Annals of R.S.C.B., ISSN:1583-6258, Vol. 25, Issue 4, 2021, Pages. 2766 – 2774
Received 05 March 2021; Accepted 01 April 2021.

reactive jammers in WSN. *IEEE Transactions on Mobile Computing*, *11*(5), 793-806.

[17] Wilhelm, M., Martinovic, I., Schmitt, J.B., & Lenders, V. (2011). Short paper: reactive jamming in wireless networks: how realistic is the threat?. In *Proceedings of the fourth ACM conference on Wireless network security*, 47-52.

[18] Ratna, S.R., Ravi, R., & Shekhar, B. (2015). An intelligent approach based on neuro-fuzzy detachment scheme for preventing jamming attack in wireless networks. *Journal of Intelligent & Fuzzy Systems*, *28*(2), 809-820. https://doi.org/10.3233/IFS-141363, in press, Sep. 2014.

[19] Thamilarasu, G., Mishra, S., & Sridhar, R. (2011). Improving reliability of jamming attack detection in ad hoc networks. *International Journal of Communication Networks and Information Security*, *3*(1), 57-66.

[20] Yang, H., Luo, H., Ye, F., Lu, S., & Zhang, L. (2004). Security in mobile ad hoc networks: challenges and solutions. *IEEE wireless communications*, *11*(1), 38-47.

[21] Djenouri, D., Khelladi, L., & Badache, A.N. (2005). A survey of security issues in mobile ad hoc and sensor networks. *IEEE Communications surveys & tutorials*, *7*(4), 2-28.

[22] Xu, W., Ma, K., Trappe, W., & Zhang, Y. (2006). Jamming sensor networks: attack and defense strategies. *IEEE network*, *20*(3), 41-47.

[23] Wood, A.D., & Stankovic, J.A. (2002). Denial of service in sensor networks. *computer*, *35*(10), 54-62.

[24] Xu, W., Trappe, W., Zhang, Y., & Wood, T. (2005). The feasibility of launching and detecting jamming attacks in wireless networks. *In Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*, 46-57.

[25] Pushpa Latha, S., & Sabitha, R. (2019). Various Jamming Attacks and Jamming Methodology: A Survey. *Journal of Advanced Research in Dynamical and Control Systems*, *11*, 04-Special Issue.

[26] Khalil, I., & Bagchi, S. (2010). Stealthy attacks in wireless ad hoc networks: detection and countermeasure. *IEEE Transactions on Mobile Computing*, *10*(8), 1096-1112.

[27] Latha, S. P., & Sabitha, R. (2016). A survey of channel allocation and attacks in multichannel multi radio wireless networks. *In Second International Conference on Science Technology Engineering and Management (ICONSTEM)*, 172-176.

[28] El Houssaini, M.A., Aaroud, A., El Hore, A., & Ben-Othman, J. (2016). Detection of jamming attacks in mobile Ad Hoc Networks using statistical process control. *Procedia Computer Science*, *83*, 26-33.