A New Approach to Mitigate Jamming Attack in Wireless Adhoc Network Using ARC Technique

Naren Tada(✉), Tejas Patalia, and Pinal Rupani

Gujarat Technological University, Chandkheda, Ahmedabad, India
naren.tada@gmail.com, pataliatejas@rediffmail.com,
rupani.pinal@gmail.com

Abstract. Wireless Adhoc Network is a set of wireless nodes that dynamically self-organizing into a changeable topology to design the network using any preceding framework. Two possibilities are there to communicate nodes; either node can communicate directly or by forwarding network traffic through intermediate nodes in wireless adhoc network. Various types of attacks can undoubtedly be accomplished by an opponent either by passing MAC layer protocol or sending Radio Signals. Reviewing the role of wireless adversary, which victims the packets of high importance and do not follow network architecture. Attacker will make possible efforts of making users not to use network resources and fail the communication. The authors believe that detecting Jamming Attack using Reactive Jammers is quite difficult. Our Proposed approach about Global Detection of Jamming is helpful in securing other nodes from Jammer's Activity by broadcasting Jammer's UID. For mitigation, our approach named ARC (Anti-Reactive Control) Technique which shows that Jamming Attack against Reactive Jammer can be detected using decreasing PDR and RSS values and successfully mitigated by executing channel hopping. Using NS3 simulation, the attack can be identified through the decreased in performance criteria and successfully mitigated by executing channel hopping. We have analyzed the result using NS3 Wireless Jamming Module.

Keywords: MANET · Jamming attack · NS-3 jamming module
Coordinated channel switching · ARC (Anti-Reactive Control) Technique

1 Introduction

Wireless adhoc network [2, 4] is a decentralized kind of wireless network. The network referred as Adhoc due to its basic characteristics such as it does not depend on a pre-existing framework, for example routers in wired network or AP in managed (framework) wifi networks. It is set of mobile nodes that can actively self-organize into a random and short-term topology to build the network. Adhoc network are constantly enhancing towards miscellaneous attacks and achieving ubiquitous computing. The common feature of wireless medium is to share and merge with commodity nature of wireless technologies and an increasingly sophisticated user-base, permits wifi network to be easily monitored and broadcast on. In Adhoc networks, each mobile node may

© ICST Institute for Computer Sciences, Social Informatics and Telecommunications Engineering 2018
Z. Patel and S. Gupta (Eds.): ICFITT 2017, LNICST 220, pp. 192–204, 2018.
https://doi.org/10.1007/978-3-319-73712-6_20

have deals directly with each other. Nodes that are not directly connected to wifi, they communicate by forwarding their traffic through relay nodes. The main benefit of Adhoc Networks is resilience, low priced and robustness. These all are qualities of adhoc network which make them well suited for military activities, emergency operations, disaster recovery, large scale community networks, and small networks. WIRELESS SECURITY [5] is the most critical attributes of Wireless communication. Mobile Adhoc Network (MANET) [2] is dynamic, independent, multi-hop network. MANET does not be in need of any fixed framework and it can be installed dynamically. Due to existence of multi-hop nature in MANET, lots of vulnerabilities present in the network. As these networks furnishing more security or more comfort zone, the issue of critical importance also come up. In MANET, different attacks such as, DDOS, Blackhole, Wormhole, Replay, Flooding, Jamming, [3] etc. have been perceived, which results in adverse effect of high level security. Since owing to fact that, Security in MANET [2, 5] is becoming challenging day by day. Attacker easily view the wireless communication between two devices and initiate simple Denial-of-Service attack against wireless network by placing distorted messages. Radio interference attacks don't seem to be available through conventional security mechanisms. An attacker will merely disregard the medium access protocol and frequently transmit on a wireless channel. On doing so, we can either intercept users to start up with legitimate MAC operations, or found packet collisions that force repeated back-offs or also jams communications.

Jamming Attack occur by continuously sending radio signals which disrupts the legitimate communication between sender and receiver. Figure 1 shows that jammer senses the communication initiated onto the wireless channel. It begins to send radio signals which injects dummy packets and receiver receives dummy packets instead of original packets send from transmitter. Attacker targets the packets of high importance. To know how jammer attacking in wireless networks and how to stay away from this jamming, researchers launch two aspects: 1. Types of existing jammers, 2. Performance Metrics. The flow of this write-up is ordered as follows: Sect. 1 incorporate an introduction to Adhoc Network, main concept and issues of MANET, Sect. 2 gives overview of Related Work, Sect. 3 gives overview Existing System, Sect. 4 shows Proposed System, Sect. 5 shows Results.

2 Related Work

2.1 Jamming Efficiency Metrics

A strong belief is there that Jammer consistently sends Radio Signals in wireless channels which results in effective blocking of channel and expected recipient might not be able to receive the message. Thus the presence of jammer in network cause interference in between legitimate communication across the wireless channel. To conclude above standards, researchers defined few metrics that apprehend the jammer's activity. Looking at the situation with one Sender (Sx) and one Receiver (Rx). Xu et al. [5] found two metrics (PSR and PDR).

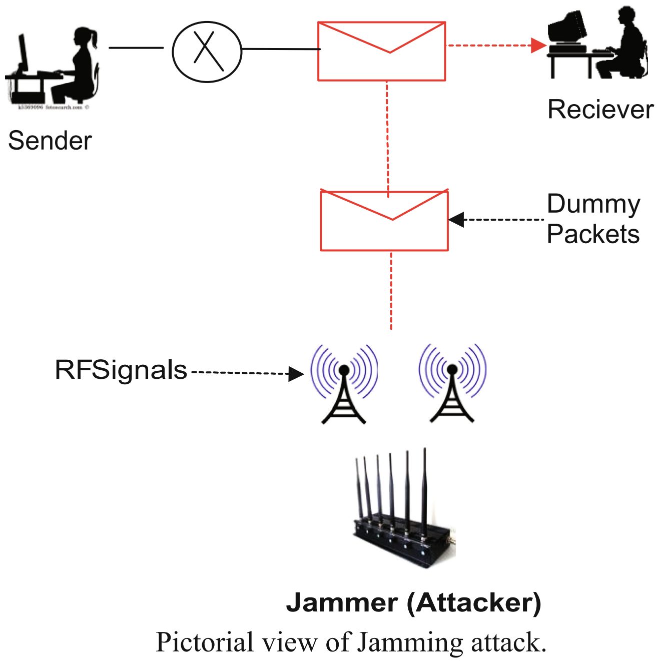

Fig. 1. Jamming attack

Packet Send Ratio (PSR) [5, 7]:
In this article, let us acquire that n number of packets transmitting through channel. Only m (n >= m) of these packets transmitted correctly.

$$PSR = \frac{m}{n} = \frac{\text{No. of Packets Sent}}{\text{Packets Observed to be Sent}} \tag{1}$$

Packet Delivery Ratio (PDR) [5, 7]:
Let's acquire that Rx receive m packets sent from Sx. But unfortunately only q of packets broadcast successfully to Rx. Packets proceed from CRC (Cyclic Redundancy Codes) check are referred as successful acceptance of Packets. If m = 0, then PDR be zero.

$$PDR = \frac{q}{n} = \frac{\text{Packets undergo CRC}}{\text{No. of Packets Received}} \tag{2}$$

2.2 Types of Jammer [5, 6, 8]:

Proactive Jammer

Proactive Jammers do not assure that any data communication is going on in wireless channel or not. This jammer keeps imparting Jamming Signals and disrupts the network. In case, some channel's status is ON; it initiates to send random bits onto that wireless channel. There are three types of proactive jammer: Constant, Deceptive and Random Jammer.

Constant Jammer

A constant jammer persistently producing radio signals on the wireless channel. The purpose of this type of jammer is dual: (a) to raise interference on any of the transmitting node in a way to distort its packets at the receiver (lower PDR) and (b) to form an authorized sender that (by using carrier sensing mechanism) sense the channel busy, thus preventing it from acquiring access to the channel (lower PSR).

Deceptive Jammer

Persistently dispatching normal packets instead of transmitting random bits (during the time of constant jammer). It misguides other nodes to assume that some genuine activity going on. As a consequence, they continue to exist in receiving states up to the time the jammer is turned off or dies. Alike to the constant jammer, deceptive jammer is energy ineffectual because of the constant transmission, but is straightforwardly executed.

Random Jammer

This Jammer periodically send either random bits or normal packets into network. Conflicting to the above two jammers, it targets to save energy. It constantly moving by linking two states: sleep and jamming phase. It sleeps for a certain amount of time and then comes in an operative/working mode for jamming before it goes back to a sleep state. The sleeping and jamming time periods are either fixed or random. There is a trade-off between jamming effectiveness and energy saving as it can't be jammed at the time of its sleeping phase. The ratios between both phase can be handled to regulate this trade-off between efficiency and effectiveness.

Reactive Jammer [5]:

Reactive jammers go ahead for jamming only when It discover some network activity arise on a few channel. It can distort small and large sized packets. After all it has to repeatedly watchdog the network; as reactive jammer is less energy efficient than random jammer. Upcoming are two different techniques to implement a reactive jammer.

RTS/CTS

It initiates jamming the network instantly when it observes that request-to-send packets transmitted from sender. As the attacker get aware that RTS packet transmitted in channel, attacker will distort this packet and thus receiver will not be able to send Clear-to-send (CTS) packet to sender. Until Sender don't get CTS response, it will send data to receiver and assumes that receiver is engaged with some other transmissions. This complete process will result in Jammer stay in standby position till CTS message sent by receiver. It will jam CTS packet when transmit from receiver which will make sender not sending data and also receiver perpetually wait for data packets to receive.

DATA/ACK
This kind jams the channel by modifying the data packets or acknowledgement (ACK) response. As per the main characteristics of reactive jammer, DATA/ACK will also not do any disruption until communication start on the channel. DATA/ACK jammers corrupt the packet when it reaches to destination and till that it will suborn packet or it will be in standby position. The alteration of both packets shows re-transmissions at the sender end. Whenever information packets were not ready to receive it exactly, they need to be retransmitted. At the time when sender does not receive ACK packets, it imagines that one thing is wrong at receiver aspect, as just in case of buffer overflow, that once more ends up in re-transmission of information packets.

2.3 Types of Jamming [18, 28]:

Physical Jamming
Physical jamming during wireless network is uncomplicated but it causes different forms of DoS attack. These attacks mainly jam the channel or network by repeatedly sending jamming signals or radio frequency signals or by sending random packets. It keeps complete control over the wireless medium. This makes waste of time as each node enter into the waiting phase and need to wait till the time jammer deactivate itself and channel becomes idle to communicates.

Virtual Jamming
The usage Virtual carrier sensing mechanism done at MAC (Media Access Control) layer. To determine the presence of jammer in network, virtual jamming plays an important role. There are several benefits of MAC layer such as rival nodes; less power consumption is there compare to physical jamming. In MAC layer, the effect of Jamming initiates by attacking on the RTS/CTS frames or DATA/ACK frames.

3 Existing System [1]

Considering scenario in which system utilizing four honest nodes in the adhoc network topology. These honest nodes named as source (node 0), recipient (node 3) and remaining two trusted relay nodes (node 1 and 2). Also one Jammer Node present in the network. The base class provide strategy to detect presence of jammer using decreasing RSS and PDR values. In this system, authors presuming that there is not any of direct link from source node to destination node for legitimate communication. Existing Jamming Strategy introduced two trusted relay nodes (act as intermediate node) to transfer message to destination. The working of their strategy begins with node 0 first transmits message to both trusted relays and then forward to destination.

The work-flow starts from Physical layer to wireless module utility whose base class imparting special functions for jamming mitigation to operate. Especially for jammer node, the strategy focuses on three different jammers': Random, Reactive and Constant. Firstly, Physical layer receive packet and forward to wireless module utility which keeps the record of packet information and calculate its RSS and PDR. After deciding on which channel jammer is activated, based on information, honest nodes request to work with different channel than one used by jammer to stay away from jamming effect.

4 Proposed System

4.1 Jamming Model

When Jammer observe that any communication initiated onto the channel, Jammer will start sending RF signal which leads to completely jammed channel. As soon as communication starts disrupting due to jamming effect, entire network nodes split into three groups named as Fully Jammed nodes, Partially Jammed Nodes and Unaffected Nodes.

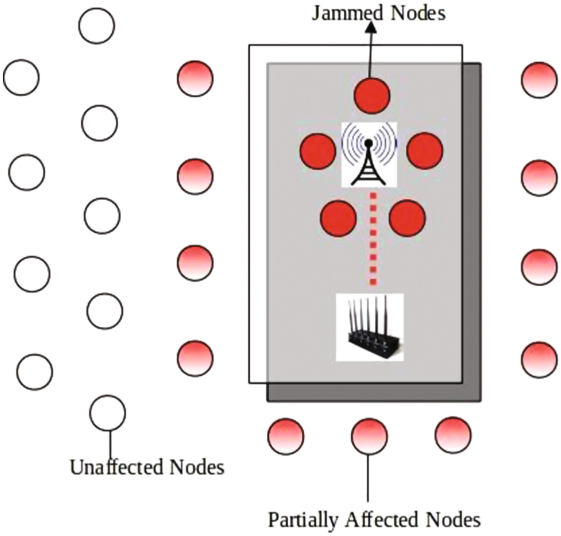

Fig. 2. Working of jamming model

As shown in Fig. 2, nodes which are nearby to jammer's position start getting affected in few seconds and ultimately it cannot receive packets from any of its neighbors. These types of nodes referred as "Fully Jammed Nodes". The area in which nodes get highly affected by jammer, declare that part as "Jammed region". Nodes which are placed at the edge of jammed region, is not completely jammed, but some part of its neighbors are jammed and referred as "Partially Jammed Nodes". This type of nodes can still reach to at least one unaffected nodes, possibly, during multi-hop nature. "Unaffected nodes" are those nodes which are placed at outermost part of the jammed region and it don't get influenced from the jamming effect.

4.2 Proposed Flowchart

See Fig. 3.

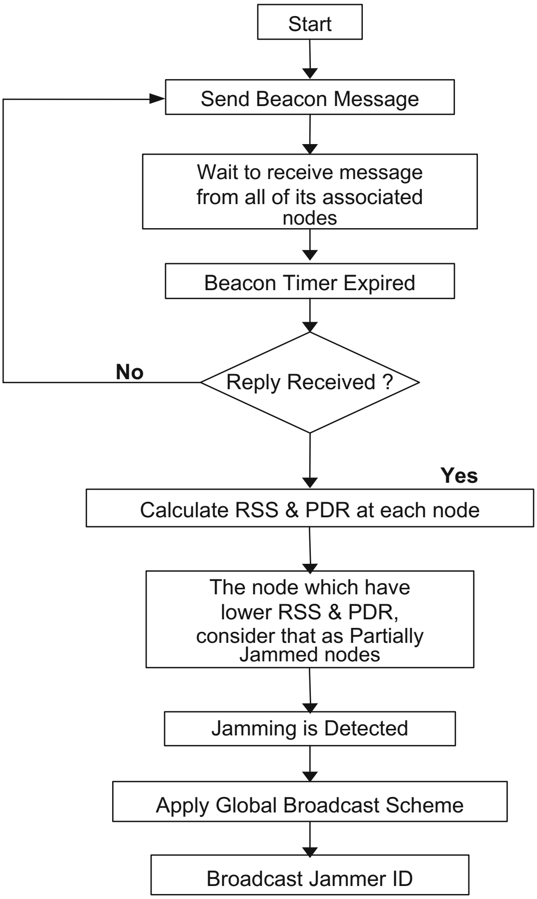
Start
Send Beacon Message
Wait to receive message from all of its associated nodes
Beacon Timer Expired
Reply Received ?
No
Yes
Calculate RSS & PDR at each node
The node which have lower RSS & PDR, consider that as Partially Jammed nodes
Jamming is Detected
Apply Global Broadcast Scheme
Broadcast Jammer ID

Fig. 3. Flowchart of Global Detection Scheme

4.3 Proposed Theory

Jamming Detection Intelligence

Asignificant amount of research has been devoted to study security issues as well as countermeasures to various attacks in MANET. However, there is still much research work needed to be done in this area. The aim to study is to mitigate Jamming Attack under Reactive Jammers in MANET. The proposed work is based on scheme for detecting the jamming effect in the network.

The proposed work is based on scheme for detecting the jamming effect in the network. For this, each and every node will have own unique ID (UID). In this scheme, after 10 s of simulation, the Base station will send Beacon Message to all of its associated nodes and wait for their beacon response. When response received by any of the nodes, we are calculating RSS and PDR values at each node. If the values are decreasing at some node, then we consider that node as Partially Jammed or Boundary Node. Thus from boundary nodes, we will declare their neighbor nodes as jammed node and jamming attack is thus detected. For Global Detection we are estimating the jammer's position and get its unique ID (UID). After finding the Jammer Unique ID, we are broadcasting message that "Do not receive packets from Jammer Unique ID". Thus we are securing all other nodes from Jammer's activity

Jamming Mitigation Intelligence
We proposed new approach referred as ARC (Anti-Reactive Control) Technique for Mitigation Strategy that comes up with base class which is Channel Hopping using Random Sequence Generator (RNG) Method. Alike in this strategy, on detection of jamming attack, channel hop scheme executes and each node shifts its current channel. As per proposed Global Detection Scheme, we are broadcasting Jammer's UID to each node which secure them from jammer's activity.

Channel Hopping [21]:
The graphical view of Channel hopping is shown in below figure. For channel hopping we are using Random Sequence Generator (RNG) Method if Channel Hop message is executed on detection of Jamming Attack. In this method, we applied logic to hop the channel based on automatic approach. This RNG method will return next channel number to switch the network nodes.

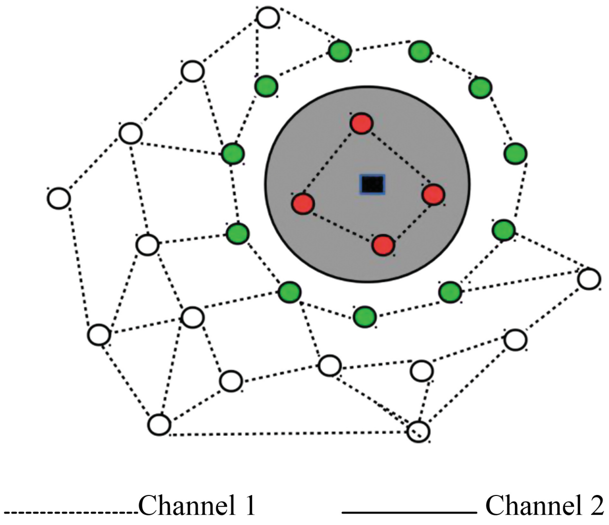

Fig. 4. Detect neighbors are not present in network (Color figure online)

Figure 4 shows that green nodes are boundary nodes of jammed area. Here nodes are realizing that their neighbors are missing from the network. After detecting that neighbors are not present in network each node will calculate its PDR and RSS value and based on results Jamming will be detected. On Detection of Jamming, RNG method will be executed and it will return next channel number to switch the communication operation.

Figure 5 shows that on execution on channel change command, each node change their channel and again start communication.

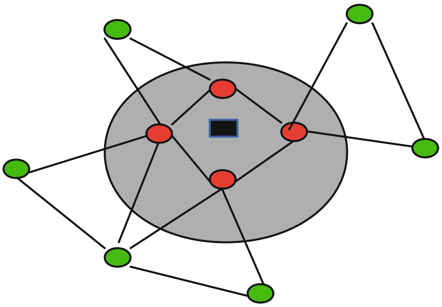

Fig. 5. Each node hops to a new communication channel

5 Results and Implementation

5.1 Implementation

Implementation of Jamming Detection and Mitigation Strategies done in NS-3 [17]. In this research we have integrated Jamming Module basically originated from https://www.nsnam.org/. To implement our strategy, we have done few modifications in the code of jamming model. All the alteration done under Reactive Jammer.

5.2 Simulation Parameters

See Table 1.

Table 1. Simulation parameters used in implementation of ARC technique

Parameter	Value
Number of packets	10000
Interval	1
Start time	0.0 s
Size of packet	100 bytes
Distance to Rx	5.0 m
Beacon port	80
Number of nodes	4 (Wifi Nodes) + 1 (Jammer Node) = 5

5.3 Results

Figure 6 shows that PDR of network. In this experiment, jammer activates node 2 and node 3 is jammed by jammer. We observed that RSS and PDR decreasing at node 2 which is boundary node. As per our results, from total simulation time of 60 s, communication stops earlier 17 s.

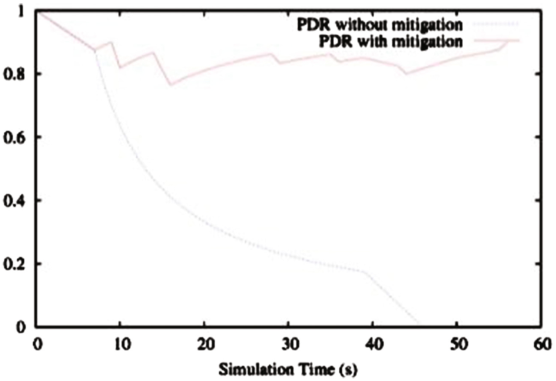

Fig. 6. PDR comparison

Figure 7. shows that RSS significantly increasing in the network as jammer's is continuously creating disturbance before implementation of ARC Technique. In 60 s of simulation RSS is not decreasing and constantly stay up to 4500 pW.

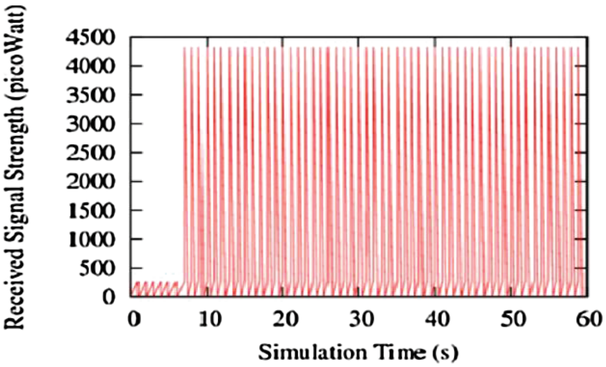

Fig. 7. RSS before mitigation

Figure 8 shows the effect of proposed mitigation strategy. It has been observed that RSS stay under pico watt.

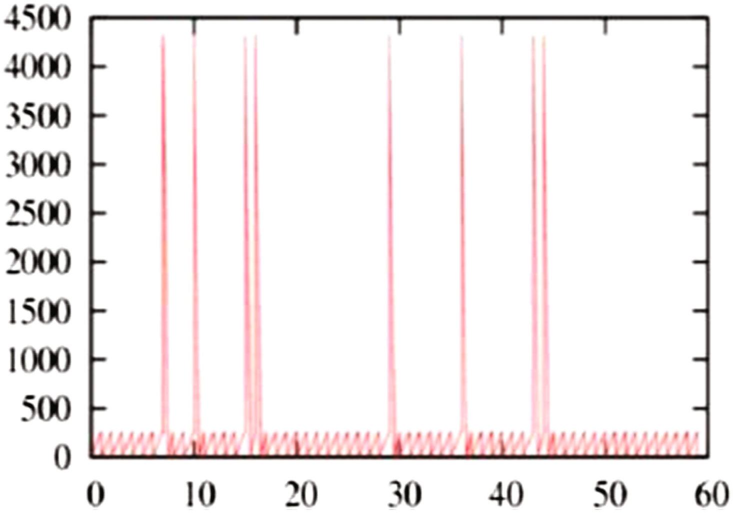

Fig. 8. RSS after mitigation

6 Conclusion and Future Scope

6.1 Conclusion

Mobile Adhoc Network (MANET) is a kind of Adhoc network with mobile, wireless nodes. Its special characteristics like open network boundary, dynamic topology and wireless communications made security highly challengeable. Jamming attack disrupts normal communication by sending continuous radio signals onto that channel.

In this research work, by studying a lot on jamming attack, we proposed new approach called ARC (Anti-Reactive Control) Technique to mitigate Jamming Attack under reactive jammers in wireless adhoc network. The proposed system will be used for Global Detection of Jamming attack and mitigating effect of jamming attack. The main advantage of our ARC Technique is “Global Broadcast Scheme”, through which we are able to secure other nodes from effect of Jamming attack from Reactive Jammers. Other main advantage is Channel Hopping using Random Sequence Generator method.

6.2 Future Scope

Overall Technique works best and fulfills its objectives but this technique works with only one Jammer. The future target is to introduce mitigation scheme by placing multiple reactive jammer’s in the network. We are hopping each node in the next channel but for future studies we should also study that only jammed node change its channel of communication.

References

1. Kushardianto, N.C., Kusnanto, Y., Syafruizal, E., Tohari, A.H.: The effect of jamming attack detection and mitigation on energy power consumption (Case study IEEE 802.11 wireless adhoc network). Jurnal Teknologi **77**, 39–46 (2015)
2. Kumari, S., Sanduja, M.R.: Detection of jamming attack in Mobile Adhoc Network. IJSETR **5**(6), June 2016
3. Kannhavong, B., Nakayama, H., Nemoto, Y., Kato, N., Jamalipour, A.: A survey of routing attacks in Mobile Adhoc Network. IEEE Wireless Commun. October 2007. Tohoku University, Sydney
4. Rubinstein, M.G., Moraes, I.M., Campista, M.E.M., Costa, L.H.M.K., Duarte, O.C.M.B.: A survey on wireless ad hoc networks. In: Pujolle, G. (ed.) MWCN 2006. ITIFIP, vol. 211, pp. 1–33. Springer, Boston (2006). https://doi.org/10.1007/978-0-387-34736-3_1
5. Pelechrinis, K., Iliofotou, M., Krishnamurthy, S.V.: Denial of service attacks in wireless networks: the case of jammers. IEEE Commun. Surv. Tutor. **13**(2), 245–257 (2011). Second Quarter
6. Grover, K., Lim, A., Yang, Q.: Jamming and anti-jamming techniques in wireless networks: a survey. Int. J. Adhoc Ubiquit. Comput. **17**, 197–215 (2017)
7. Xu, W., Ma, K., Trappe, W., Zhang, Y.: Jamming sensor network: attack and defense strategies. IEEE Network **20**, 41–47 (2006)
8. Xu, W., Trappe, W., Zhang, Y., Wood, T.: The feasibility of launching and detecting jamming attacks in wireless networks. Wireless Information Network Laboratory (WINLAB) Rutgers University, 73 Brett Rd., Piscataway, NJ 08854, 25–27 March 2005
9. Naren, T., Tejas, P., Chirag, P.: Trust appraisal based neighbour defense secure routing to mitigate various attacks in most vulnerable wireless ad hoc network. In: Satapathy, S.C.C., Das, S. (eds.) Proceedings of First International Conference on Information and Communication Technology for Intelligent Systems: Volume 1. SIST, vol. 50, pp. 323–332. Springer, Cham (2016). https://doi.org/10.1007/978-3-319-30933-0_33
10. Popli, P., Raj, P.: Mitigation of jamming attack in Mobile Adhoc Network. IJIRCCE **4**(6) (2016)
11. Popli, P., Raj, P.: Securing MANET by eliminating jamming attack through mechanism. IJSETR **5**(9), September 2016
12. Liu, H., Liu, Z., Chen, Y., Xu, W.: Determining the position of a jammer using a virtual-force iterative approach. Wireless Netw. **17**, 531–547 (2010). Springer Publication
13. Misra, S., Dhurandher, S.K., Rayankula, A., Agrawal, D.: Using honeynodes for defense against jamming attacks in wireless infrastructure-based network. Comput. Electr. Eng. **36**, 367–382 (2009). Elsevier
14. Vijayakumar, K.P., Ganeshkumar, P., Anandaraj, M.: Jamming detection system in wireless sensor networks. IJARCET **3**(4), April 2014
15. Liu, H., Xu, W., Chen, Y., Liu, Z.: Localizing jammers in wireless network. Dept of ECE, Stevens Institute of Tech. Castle Point on Husdon, Hoboken, NJ 07030 and Dept of CSE, Uni. Of South Carolina, Columbia, SC 29208
16. Popli, P., Raj, P.: Effect of jamming attack in Mobile Adhoc Environment. IJSETR **5**(5), May 2016
17. Khosla, H., Kaur, R.: Jamming attack detection and isolation to increase efficiency of the network in Mobile Ad-Hoc Network. IJRET **2**(4), July 2015
18. Liu, Z., Liu, H., Xu, W., Chen, Y.: Exploiting jamming - caused neighbor changes for jammer localization. IEEE Trans. Parallel Distrib. Syst. **23**(3), 547–555 (2012)

19. Xu, W., Wood, T., Trappe, W., Zhang, Y.: Channel surfing and spatial retreats: defense against wireless denial of service. In: Proceedings of ACM Wireless Security, 1 October 2004
20. Ajana, J., Helen, K.J.: Mitigating inside jammers in MANET using localized detection scheme. IJESI **2**(7), 13–19 (2013)
21. Zhang, R., Sun, J., Zhang, Y., Huang, X.: Jamming-resilient secure neighbor discovery in Mobile Ad Hoc Networks. IEEE Trans. Wireless Commun. **14**, 5588–5601 (2015)
22. Thuente, D., Acharya, M.: Intelligent jamming in wireless networks with applications to 802.11b and other networks. IEEE
23. Mpitziopoulos, A., Gavalas, D., Konstantopoulos, C., Pantziou, G.: A survey on jamming attacks and countermeasures in WSNs. IEEE Commun. Surv. Tutor. **11**(4) (2009). Fourth quarter
24. Thamilarasu, G., Mishra, S., Sridhar, R.: A cross-layer approach to detect jamming attacks in wireless ad hoc networks. IEEE
25. Ben-Othman, J., Hamieh, A.: Defending method against jamming attack in wireless ad hoc networks. IEEE, 20–23 October 2009
26. Hamieh, A., Ben-Othman, J.: Detection of jamming attacks in wireless ad hoc networks using error distribution. IEEE (2009)
27. Ashraf, Q.M., Habaebi, M.H., Islam, M.R.: Jammer localization using wireless devices with mitigation by self-configuration. PLoS One (2016)
28. Chaturvedi, P., Gupta, K.: Detection and prevention of various types of jamming attacks in wireless networks. IJCNWC **3**(2), 2250–3501 (2013)
29. Kopena, J.: Wireless Jamming Model. https://www.nsnam.org/wiki/Wireless_jamming_model
30. NS3 Official Site: https://www.nsnam.org/