Security and Efficiency Analysis of Anti-jamming Techniques

S. Kshipra Prasadh and Sumit Kumar Jindal(✉)

School of Electronics Engineering, Vellore Institute of Technology, Vellore, Tamil Nadu, India
sumitjindal08@gmail.com

Abstract. Internet of Things has resulted in ubiquitous computing, where all IoT devices are connected almost all the time, to provide continuous services. This makes the network prone to several attacks, one such attack being the Direct Denial of Service (DDoS) attack. Jamming, which is the use of malicious nodes to deliberately lower Signal to Noise ratio (SNR), is a subset of DDoS attacks, which affects physical layer devices and channels, and can cause errors in the upper layers. Anti-jamming techniques, which are used to mitigate the effects of jamming, must be analyzed from the security and efficiency perspective. In this paper, anti-jamming techniques and protocols, viz. JAM- Jammed Area Mapping, Channel surfing and spatial retreat, channel hopping, reactive jamming detection and trigger node detection; are compared with respect to security and efficiency parameters. The suitable techniques are finally selected for specific use cases.

Keywords: Jamming · Device layer · Signal to noise ratio · Nodes · Bit error rate · Collision

1 Introduction

With the advent of Internet of Things, several functions have been automated. However, for achieving real time operations and continuous automation, the devices have to be connected to the internet all the time. This makes IoT devices prone to many security threats and attacks [1]. One such security threat is called the Direct Denial of service (DDoS) attack. Here, the communication of packets from the source to the destination is prevented. This could be done without the user's knowledge, deliberately, to reduce the performance of the wireless network. Jamming is a type of DDoS attack, which can cause security threats to the upper layers too.

Jamming can be intentional or unintentional. Sometimes, the nodes present in a network may jam the network. This is reduced by reducing the traffic or by reducing the number of nodes. Jamming is intentionally done by hackers, who wish to prevent communication in wireless networks, by reducing the signal to noise ratio at the transmitting or receiving end. Jamming can be done either by adding malicious nodes, to disrupt communication, or using multiple wireless signals to confuse the channel. Jamming is also done by distorting packet information, like the headers, trailers, message, checker bits, etc. so the packet either contains wrong information or it is routed to the wrong

N. Nain and S. K. Vipparthi (Eds.): ICIoTCT 2019, AISC 1122, pp. 251–259, 2020.
https://doi.org/10.1007/978-3-030-39875-0_27

node. Jamming attacks are hard to detect, and can be detected only after considerable number of packets have been lost or damaged [2]. This makes usage of anti-jamming techniques a necessity in almost every IoT system.

The working of jammers can be realized by estimating the types of jammers, the protocols used in jammers, and the anti-jamming techniques available to counter the effects of jamming. Anti-jamming techniques need to be analyzed based on the efficiency of the technique. The algorithms must have the least execution time and must provide real-time protection against jamming. They must also be able to detect the presence of malicious nodes and signals within a very short period of time. Another important aspect of anti-jamming algorithms is security. Anti-jamming algorithms must be secure themselves, and should not be accessible to the intruder, lest they would become ineffective. There are several techniques for the detection and prevention of jamming. They include channel surfing and spatial retreat, channel hopping, reactive jamming detection, trigger control detection and the use of Hermes nodes. In this paper, all the anti-jamming algorithms are compared with respect to efficiency and security.

The wireless network scenario was deployed in NETSIM ACADEMIC V2.0. For each of the techniques, the MATLAB code was interfaced with NETSIM, to analyse the functioning of the protocol. The application and network metrics were analyzed to determine the throughput, number of packets collided and number of packets transmitted. The security analysis was done based on the MATLAB code.

The paper is divided as follows. Section 2 describes the different jamming techniques and protocols. Section 3 describes the anti-jamming techniques. Section 4 highlights the simulation and results.

2 Jamming Techniques

Jammers are always seen as a threat to physical layer security. However, it has been proved that jammers can also be useful. A node can jam itself, so that it can prevent external attacks. As a threat, jammers are used to send wireless signals continuously over a radio channel, and this utilizes the complete capacity of the channel. Hence, any transmitter that wants to transmit legitimate data is forced to back off, and the transmission of meaningful data is prevented. There are different types of jammers. Jammers are classified based on their point of attack. Some jammers attack nodes, by preventing them from transmitting data. Some attack the wireless channel, by flooding it with unnecessary signals. Some attack the packets, modifying the packet information [3–7].

Jammers are classified as simple or complex, based on their operation and usage. Simple jammers do not use complex jamming algorithms. They just send packets over the wireless channel. Simple jammers are further classified into proactive and reactive jammers.

Proactive jammers- These jammers keep sending data on the radio channel, until it dies out. The effect of continuous transmission is that the other nodes are unable to transmit their packets, as the radio channel is already engaged. There are three types of proactive jammers- Constant jammer, deceptive jammer and random jammer [8].

Constant jammers send random bits of data across the channel. The other nodes in the network are made to believe that transmission of data is taking place, and hence, they

are switched off. This technique is easy to deploy, but is also easy to detect. Deceptive jammers, on the other hand, send continuous streams of data, thus masquerading legitimate communication. The other nodes are in their 'receive state' till the jammer sends data and is drained of energy. They are harder to deploy and harder to detect, as continuous streams of data are sent, instead of random packets. A random jammer combines the principles of the deceptive and constant jammers. It either sends random packets, or continuous steams of data, or does not send any data, depending on the network situation. It makes random decisions on the type of packets to be sent.

Reactive Jammer- Unlike a proactive jammer, which sends data even when no nodes communicate, a reactive jammer starts its operation only when it senses some form of communication in the network. The receiving nodes are blocked, and thus a reactive jammer prevents packets from being received. There are many ways a reactive jammer operates. One such method is by preventing the 'send request' from the sender. Then, the receiver does not send the 'Send' command. So, the sender assumes the receiver is busy and switches off operation. Another technique is to damage the ACK packets, which are sent from the receiver to the sender on the successful receipt of data packets. When the acknowledgement packets are damaged, the sender re-sends the packet again and again till it receives a positive acknowledgement. This causes the network to jam [9].

Complex jammers work on multiple channels, and use concepts of single jammers, in order to produce a complex jamming technique, which makes it very hard to detect the kind of jamming technique that is being used. Some complex jammers are function specific. These jammers make use of a predefined algorithm, so as to perform a specific function, without the unnecessary wastage of packets. This helps the jammer to extend its battery life. Such jammers can be follow- on type, channel hopping type or pulsed noise type. In follow on type, the jammer switches between multiple channel randomly, whereas in channel hopping type, the jammer follows an algorithm to jump between channels [10–12].

Certain jammers are given intelligence, and are able to take real- time decisions as to which channel has to be attacked. These jammers are the hardest to detect. Some jammers may, in addition to distorting packets, damage some nodes, thus switching off the node permanently. Some jammers specifically damage the control channels in a system, thus destroying all the important transmission related information. Others may cause Denial of service attacks [13].

Thus, jamming techniques are becoming more complex by the day and detection of jamming plays a very important role in any IoT system.

3 Anti-jamming Techniques

To counteract the given jamming techniques, several anti-jamming algorithms are used. First, the network scenario is deployed using NETSIM ACADEMIC v2.0. Then the algorithms are coded in MATLAB and interfaced with NETSIM. The throughput, number of packets transmitted and collided are determined from NETSIM. Based on the above information, the efficiency of the algorithm is determined. The anti-jamming techniques studied in this paper are as follows.

3.1 JAM- Jammed Area Mapping (JAM)

This protocol is used to map the jammed area. The mapping is used to determine the jammed and non-jammed paths. Once the paths are determined, the packets are routed between non-jammed paths, around the jammed paths. This protocol helps in successful transmission of the packets, but results in a lot of packet collisions and reduces the throughput of the network. This method does not counter jamming, instead avoids it. Hence, the physical layer is still prone to attacks [13].

3.2 Channel Surfing and Spatial Retreat (CSSR)

Channel surfing moves to another channel when a jammer attacks a channel. The next channel is determined by considering all the orthogonal channels in the wireless network and identifying the free or available channel among all the channels. Spatial retreat involves transferring the nodes from a jammed region to a safer region. Channel surfing requires a quite complex algorithm and additional security needs to be implemented in the algorithm. Without security, the channel surfing algorithm can be accessed and modified by the intruder. In spatial retreat, the entire network has to be reconfigured, as the nodes need to be moved from one part of the network to another.

3.3 Channel Hopping (CH)

Channel hopping involves shifting from one channel to another. While channel hopping may seem a suitable counteractive measure, handoff requests from users, especially in ad hoc networks, severely limit the performance of this technique. Hence, channel hopping is not very suitable for ad-hoc networks. One type of channel hopping involves shifting from one channel to another irrespective of whether there is jamming or not. Another type of channel hopping sets a jamming threshold ‘a’, and if the jamming is more than ‘a’, the next channel is utilized.

3.4 Reactive Jamming Detection (RJD)

This technique uses the strength of the signal of the received bit to determine the presence of jamming. If the strength is low and the bit is distorted, then it is due to internal packet collisions. If the strength is high, but the packet is distorted, it is due to jamming. Reactive jamming detection is easier to implement and reduces the amount of packet collisions [14].

Another technique followed here is the trigger node detection. Here, the nodes which trigger the reactive jamming are identified. First, the entire network is scanned and the harmless nodes are first detected. The information about the harmless nodes are sent to the base station. Second, the triggered nodes which are controlled by the jammer are detected and separated from the other nodes. Then, all the triggered nodes are switched off [15].

4 Results and Discussion

The wireless network scenario was deployed in NETSIM. The IoT scenario is deployed using wireless sensor networks. 16 nodes are deployed in an area of 100 * 100 m^2. Out of these, Node 5 is defined as the jamming (malicious) node. The MATLAB codes for the anti-jamming techniques are interfaced with the NETSIM code.

The block diagram of the above system is given in Fig. 1. A constant simulation time of 100 s was used for all the cases. The default link speeds of 10 m/s uplink and downlink was used and the nodes were arranged in a random order.

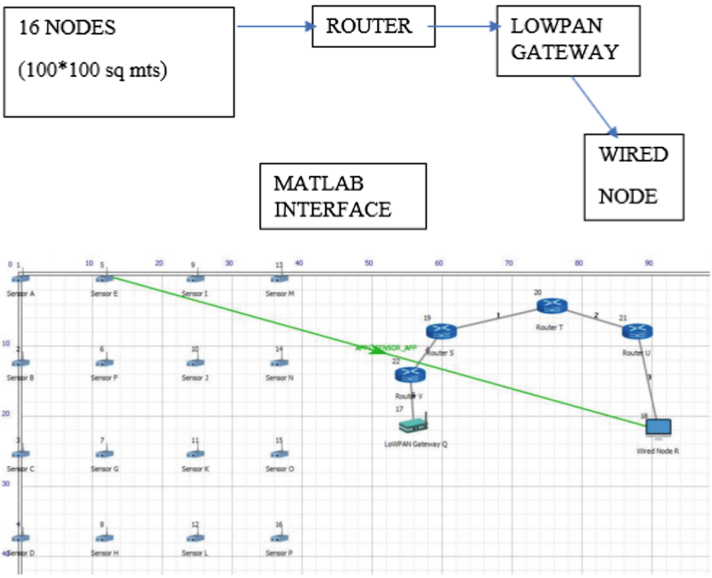

Fig. 1. Network diagram of the WSN system

The router is a network layer device, which transmits packets to the LOWPAN gateway. The MATLAB code is interfaced with the wireless channel between the 16 nodes and the router. It performs the desired modifications to the channel and to the entire NETSIM environment, to eliminate jamming.

The three main parameters which determine the efficiency of any protocol are the throughput, the number of packets collided and the number of packets transmitted. Throughput of any network is the number of packets transmitted successfully from the sender to the receiver. It is measured in Mbps or Kbps. It denotes how effective a protocol is, in terms of routing of packets.

4.1 Throughput

Reactive Jamming Detection technique has the highest throughput, as the trigger node is identified and turned off. Channel spacing and Spatial retreat (CSSR) has the second highest throughput, as it effectively removes a node from the jammed area and places it in an non-jammed region. JAM has the third highest throughput, as it only maps the area, without effectively preventing jamming. Channel hopping causes much more packet collisions, especially in band-limited environments, hence, it has the least throughput. Table 1 shows the throughput values obtained from the network metrics and Fig. 2 shows the graph obtained from the NETSIM plot.

Table 1. Throughput (in Kbps) of the different techniques

JAM	12.8667
CSSR	15.2456
CH	9.8767
RJD	23.4656

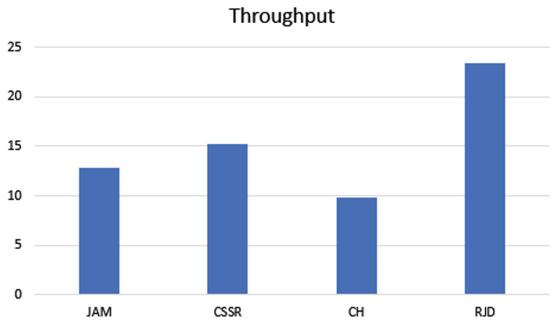

Fig. 2. Throughput (in Kbps) of the different techniques

4.2 Number of Packets Transmitted

Reactive Jamming Detection technique has the highest number of packets transmitted, as the jamming is prevented at an early stage itself. Channel spacing and Spatial retreat (CSSR) has the second highest packets transmitted, as packets are routed to a different area. JAM has the third highest throughput, as it only maps the area, but causes collision of packets, as it leads to congestion of packets in areas around the jammer. Channel hopping causes much more packet collisions, especially in band-limited environments, hence, it transmits the least number of packets. Table 2 shows the number of packets transmitted obtained from the network metrics and Fig. 3 shows the graph obtained from the NETSIM plot [16].

Table 2. Number of packets transmitted for the different techniques

JAM	2864
CSSR	3678
CH	1345
RJD	3989

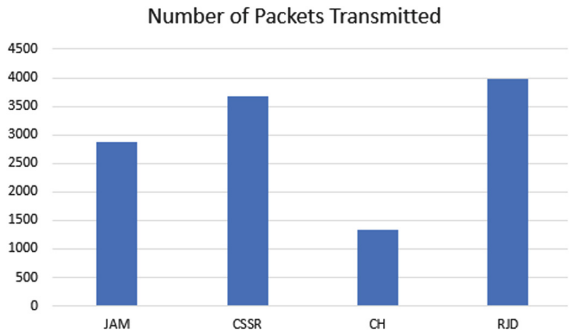

Fig. 3. Number of packets transmitted for the different techniques

4.3 Number of Packets Collided

Reactive jamming detection has the least number of packets collided, as the technique prevents jamming. Jammed area mapping has the maximum number of packets collided, as the protocol leads to congestion in the network. Channel hopping also causes packet collision, due to excess traffic in neighbouring channels. CSSR reduces the amount of collisions, due to selective channel hopping. Table 3 shows the number of packets collided, obtained from the network metrics and Fig. 4 shows the graph obtained from the NETSIM plot.

Table 3. Number of packets collided for the different techniques

JAM	258
CSSR	125
CH	212
RJD	67

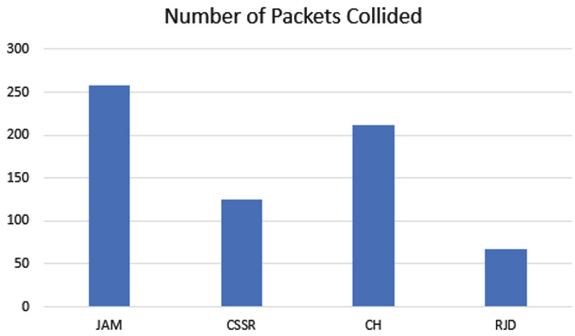

Fig. 4. Number of packets collided for the different techniques

4.4 Security Analysis

Some anti-jamming algorithms require additional security to prevent intruders from modifying the technique and weakening the protection against jamming. Among the algorithms analyzed, channel surfing algorithm requires the maximum security, as a modification in the algorithm can change the entire network scenario. Encryption keys need to be implemented to allow access to the code. If not properly implemented, intruders can change the channel surfing methodology and increase traffic in all channels. Channel hopping does not require much security as it is proactive, and does not follow a specific algorithm. However, if reactive jamming technique is applied, high security has to be provided, as the intruder can turn off victim nodes, if the algorithm is accessed. Hence, the reactive jamming technique algorithm must be accompanied by strong RSA encryption or elliptical curve encryption techniques to avoid turning off the victim nodes. If the JAM protocol is secure in a network, there can be denial of service attacks in the network, where require packets are lost in their path to the destination.

5 Conclusions

In this work, the efficiency and security of the anti-jamming techniques are analyzed and compared. The efficiency is analyzed in terms of throughput, number of packets transmitted and collided. It is found that the reactive jamming protocol has the maximum throughput, and transmits the maximum number of packets in a given time and causes least packet collisions. However, excessive security needs to be provided to this technique, as if the intruder has access, the harmless victim nodes can be turned off instead of the malicious trigger node. The channel hopping technique is very easy to implement, but has the least throughput and causes lots of packet collisions, as the technique just involves proactive switching between adjacent channels. Channel surfing and spatial retreat algorithm is quite complex, and has a run-time of $O(n^2)$. However, the algorithm is effective against most of the jamming techniques available, including smart jamming. It performs reactive channel hopping and hence reduces the number of packet collisions. However, due to the problem of multiple handoff requests, this technique cannot be used for ad hoc networks.

References

1. Alnifie, G., Simon, R.: A multi-channel defense against jamming attacks in wireless sensor networks. In: Proceedings of the 3rd ACM Workshop on QoS and Security for Wireless and Mobile Networks, pp. 95–104 (2007)
2. Bayraktaroglu, E., King, C., Liu, X., Noubir, G., Rajaraman, R., Thapa, B.: On the performance of IEEE 802.11 under jamming. In: IEEE the 27th Conference on Computer Communications, pp. 1265–1273 (2008)
3. Bellardo, J., Savage, S.: 802.11 denial-of-service attacks: real vulnerabilities and practical solutions. In: Proceedings of the 12th Conference on USENIX Security Symposium, pp. 15–28 (2003)
4. Broustis, I., Pelechrinis, K., Syrivelis, D., Krishnamurthy, S.V., Tassiulas, L.: FIJI: fighting implicit jamming in 802.11 WLANs. In: Security and Privacy in Communication Networks, vol. 19, pp. 21–40 (2009)
5. Chiang, J.T., Hu, Y.C.: Cross-layer jamming detection and mitigation in wireless broadcast networks. IEEE/ACM Trans. Netw. **19**(1), 286–298 (2011)
6. Commander, C.W., Pardalos, P.M., Ryabchenko, V., Shylo, O.V., Uryasev, S., Zrazhevsky, G.: Jamming communication networks under complete uncertainty. Optimization Letters **2**(1), 53–70 (2008)
7. Gencer, C., Aydogan, E.K., Celik, C.: A decision support system for locating VHF/UHF radio jammer systems on the terrain. Information Systems Frontiers **10**(1), 111–124 (2008)
8. Gollakota, S., Katabi, D.: iJam: jamming oneself for secure wireless communication. Technical report, Massachusetts Institute of Technology (2010)
9. Andrea, I., Chrysostomou, C., Hadjichristofi, G.: Internet of Things: security vulnerabilities and challenges. In: 2015 IEEE Symposium on Computers and Communication (ISCC), 6 July 2015, pp. 180–187. IEEE (2015)
10. Aman, M.N., Chua, K.C., Sikdar, B.: Position paper: physical unclonable functions for IoT security. In: Proceedings of the 2nd ACM International Workshop on IoT Privacy, Trust, and Security, 30 May 2016, pp. 10–13. ACM (2016)
11. Fang, H., Xu, L., Zou, Y., Wang, X., Choo, K.K.: Three-stage Stackelberg game for defending against full-duplex active eavesdropping attacks in cooperative communication. IEEE Trans. Veh. Technol. **67**(11), 10788–10799 (2018)
12. Bharathi, S., Kumar, D., Ram, D.: Defence against responsive and non-responsive jamming attack in cognitive radio networks: an evolutionary game theoretical approach. J. Eng. **2018**(2), 68–75 (2018)
13. Chen, Y., Li, Y., Xu, D., Xiao, L.: Dqn-based power control for IoT transmission against jamming. In: 2018 IEEE 87th Vehicular Technology Conference (VTC Spring), 3 June 2018, pp. 1–5. IEEE (2018)
14. Bany Salameh, H., Almajali, S., Ayyash, M., Elgala, H.: Spectrum assignment in cognitive radio networks for Internet-of-Things delay-sensitive applications under jamming attacks, 2327–4662. https://doi.org/10.1109/JIOT.2018.2817339
15. Garnaev, A., Trappe, W., Petropulu, A.: An anti-jamming strategy when it is unknown which receivers will face with smart interference. In: International Conference on Wired/Wireless Internet Communication 18 June 2018, pp. 195–206. Springer, Cham (2018)
16. Bany Salameh, H., Almajali, S., Ayyash, M., Elgala, H.: Batch-based security-aware spectrum sharing with simultaneous assignment decisions in time-critical IoT networks with cognitive radio capabilities. Trans. Emerg. Telecommun. Technol. **29**(11), e3317 (2018)