World Academy of Science, Engineering and Technology
International Journal of Computer and Information Engineering
Vol:9, No:2, 2015

Survey on Jamming Wireless Networks: Attacks and Prevention Strategies

S. Raja Ratna, R. Ravi

Open Science Index, Computer and Information Engineering Vol:9, No:2, 2015 publications.waset.org/10003033/pdf

***Abstract*—**Wireless networks are built upon the open shared medium which makes easy for attackers to conduct malicious activities. Jamming is one of the most serious security threats to information economy and it must be dealt efficiently. Jammer prevents legitimate data to reach the receiver side and also it seriously degrades the network performance. The objective of this paper is to provide a general overview of jamming in wireless network. It covers relevant works, different jamming techniques, various types of jammers and typical prevention techniques. Challenges associated with comparing several anti-jamming techniques are also highlighted.

***Keywords*—**Channel, Cryptography, Frequency, Jamming, Legitimate, Security, Wavelength.

I. Introduction

SECURITY issues and attack management have become prime importance for communication in wireless networks. Due to the broadcast nature of the wireless medium, wireless networks are highly vulnerable to attacks. There are many different attack strategies an adversary can use to disturb wireless communications. One of the most effective attacks on wireless networks is Denial-of-Service (DOS) attack. Jamming attack is a sub class of DOS attack [3], [6], [7], [9], [28], [36], [53]. DOS intensely attempt to prevent legitimate users from reaching a specific network resource. This paper focuses on jamming attack. Jamming attack intentionally disrupts the network service.

Jammer [3], [4] is an entity who is purposefully trying to interfere with the physical transmission and reception of wireless communications. The objective of jamming attack [16] is to prevent a legitimate sender or receiver from transmitting or receiving packets. A jammer may either corrupt control packets or reserve the channel for the maximum allowable number of slots, so that other nodes experience low throughput by not being able to access the channel [13], [54]. Jammer either continuously emits signal on the channel so that the sender will always sense the channel as busy or sends regular data packets and forces the receiver to receive junk packets all the time. In the latter case, the sender successfully sends the packets to the receiver, but the jammer blast a radio transmission to corrupt the message that the receiver receives.

Jamming disrupt wireless transmission unintentionally either in the form of interference, noise or collision at the receiver side [12]. It overpowers the transmitted signals by injecting high level of noise which lowers the signal-to-noise ratio, thereby reducing the probability of successful packet reception [23]. An ideal jamming attack [5] should have high energy efficient, reduced probability of detection, resistant to anti jamming techniques and also disrupts the communications to maximum possible extent.

The paper proceeds as follows. Section II describes attack analysis and different types of jammers. Section III explains the comparison of various anti jamming techniques. Finally, Section IV concludes the paper.

II. Attack Analysis

Communication security is correlated to two features, system reliability and message secrecy. Transmission of secret message to a legitimate receiver under certain conditions is known as message secrecy. The enemy of message secrecy is eavesdropper [1], [2], [27], [78]. If a certain encoded message intended for a specific legitimate receiver is reliably received by that receiver, it is known as system reliability. The enemy of system reliability is jammer [16], [65].

A. Active and Passive Attacks

Attacks can be categorized as active or passive. Passive attackers does not send any message, but just listens to the channel and also steal the packets containing IP addresses, location of nodes, etc. They do not disrupt communication or cause any direct damage to the network, but seek information and violates the network confidentiality. An example is eavesdropping. The sole purpose of an eavesdropper is to listen to the transmission and to obtain some confidential information that should be kept secret during communication. The confidential information includes the location, public key, private key, or even passwords of the nodes [25].

Active attackers disrupt the normal operation of a specific node or target the operation of the whole network. Active attacker performs injecting of packets to wrong destinations, dropping of packets, deleting packets and modifying the contents of packets which violate availability, integrity, authentication, and non-repudiation paradigm. An example is jamming attack. Active attackers like eavesdroppers can be prevented using cryptographic measures whereas passive attackers like jammers are hard to detect and prevent [24].

S. Raja Ratna is a full time Research Scholar with the Anna University recognized Research Center in Francis Xavier Engineering College, Tirunelveli, Tamil Nadu 627003 India (phone: 91 9486938282; fax: 0462-2501007; e-mail: gracelinrr@yahoo.com).

Dr. R. Ravi is dean with the Computer Science and Engineering Research Department, Francis Xavier Engineering College, Tirunelveli, Tamil Nadu 627003 India (e-mail: csehod@francisxavier.ac.in).

Open Science Index, Computer and Information Engineering Vol:9, No:2, 2015 publications.waset.org/10003033/pdf

B. Internal and External Attacks

Jamming attack in wireless network falls under the following two categories [26], external attack [10], [28], [69] and internal attack [8], [43], [49], [61], [73], [77], [79]. In external attack, the jammer lies outside the network and is not a part of the network. It may either cause congestion or propagate fake routing information or disturb the nodes from providing services. In internal attack, the jammer becomes a part of the network knowing all network secrets and participates in various malicious activities.

C. Classification of Jamming Attack

There are two classifications of jamming attack, PHY jamming/RF jamming and MAC layer/Virtual jamming. Jamming is usually aimed at the physical layer, but they may also be occurred at the MAC layer [10]-[14], [22], [54].

Jamming at the physical layer is PHY jamming [15]. In PHY jamming [74], the jammer sends high power signal to cause extremely low SNR ratio at legitimate receiver, thereby corrupting the communication link. It is launched by continuous transmissions or by causing packet collisions at the receiver side. The goal of this jamming is to distort the legitimate signal by sending unwanted signals or noise on the same radio channel, thereby preventing proper reception of the signal at the receiver [45].

Jamming at the medium access control layer is MAC jamming. MAC jamming attacks either the control frames or data frames. The jammer [12], [13], [20] disrupts the legitimate user's packet transmission by sending jamming packets on the RTS/CTS frames or DATA frames [17], [18]. A significant advantage of MAC jamming is that the attacker node consumes less power in targeting these attacks when compared to PHY jamming.

D. Jamming Methods

Generally one of the following four jammers is used for jamming. The jamming models [3], [19], [21] in PHY jamming are constant, deceptive, random, and reactive.

1. Constant Jammer

Constant jammer constantly emits random meaningless noise signals on the wireless medium and it will not wait for the channel to be idle before transmitting.

2. Deceptive Jammer

Deceptive jammer constantly injects regular packets of noise signal with no gap between them. Deceptive jammer is similar to constant jammer [3]; the similarity between the two is that both continually emit noise signals. The main difference them is that constant jammer continuously emits random noise signal, whereas the deceptive jammer continually emits noise signal on the channel without any gaps between the transmissions. Therefore, the user believes that some legitimate transmission is going on. Deceptive jamming is harder to detect than constant jammer. Both constant and deceptive jamming hinders the transmission and target transmission at the receiver side. One disadvantage of both the jammers is their power efficiency, because the signal is emitted continuously on the channel, their power efficiency is poor.

3. Random Jammer

A random jammer randomly emits noise signal on the wireless medium and considers energy conservation. For a random period of time the jammer behaves like constant jammer or deceptive jammer and then remains ideal for another random period of time. Main advantage of this jammer is that it saves energy which is very important.

4. Reactive Jammer

Of the four jammers, the smarter and most power efficient one is the reactive jammer which targets the reception of a packet and deterministically jams only when the communication medium is busy [30]-[35]. This jammer remains quiet until there is activity on the channel, it constantly senses the channel and when it finds packet transmission it immediately transmits radio signal and causes collision at the receiver side. Reactive jammer spent more energy for sensing the channel and spends little energy to interrupt the packet. It takes smarter jamming decision. Detection of this jamming is very challenging because it minimizes the risk of exposure. Its network performance does not degrade heavily; the overall throughput under reactive jammer is higher than the throughput obtained against other jammers

III. Comparison of Anti Jamming Techniques

Recovery from jamming attack requires an efficient prevention mechanism. In wireless network, prevention approaches are more important because an efficient approach can increase the network performance. Existing jamming prevention techniques are wavelength assignment [37], [38], [62], Channel surfing [39], [40], [52], [63], [70], Game theory approach [41], [44], [46], [51], [71], Zonalization [42], Trigger identification [33], Frequency hopping [23], [29], [47], [50], [60], [64], [68], [73], [75], Threshold based technique [31], [48], Cryptographic key distribution [56], [66], Detection based prevention [58], [67], Multi path routing [55], [57], [59], Packet hiding [27], [72], [76].

A. Channel Surfing

Channel surfing is an effective method to prevent jamming attack in wireless communications. Two parties have to negotiate beforehand, in order to agree on the channel switching sequence. Different channel surfing techniques are listed in Table I.

B. Wavelength Assignment

Deliberate high powered jamming attack seriously degrades the network performance and must be dealt efficiently. One of the most important challenges in preventing jamming attack is successfully solving using routing and wavelength assignment problem. Different wavelength assignment techniques are listed in Table II.

TABLE I
CHANNEL SURFING

Technique	Description	Advantages	Disadvantages
Neighbour based proactive channel hopping [39]	Each node has a designated control channels. They communicate with its neighbours on different channels and are dynamically coordinated between them.	Efficient as compared to other proactive schemes.	Efficiency reduces if burst of packets are exchanged between pairs of nodes.
Channel Surfing without prior negotiation [40]	Wireless fading channel state is used as a random shared secret between legitimate parties to achieve channel agreement. Provides jamming-resistant communication.	No extra communication overhead. Strong security and robust.	Performance degrades when two parties use different transmission power.
Defence using honey nodes and Channel surfing algorithm [52]	Jamming attack is prevented using honey nodes, along with an attack response mechanism based on Channel Surfing strategy to resist jammers.	Achieve better robustness. Packet delivery ratio is better than channel surfing.	Works well only for infrastructure-based networks and not for ad hoc networks.
Channel aware detection algorithm [63]	Identify misbehavior from normal channel losses based on channel estimation and traffic monitoring.	Detects attackers efficiently. Increase packet delivery ratio.	Does not deal with multiple malicious nodes in collision.
Adaptive Rapid Channel Hopping [70]	Uses Dwell Window and each channel's transmission time is adjusted based on the jammer's ability.	Increases network throughput.	Could not overcome sophisticated smart jammers.

TABLE II
WAVELENGTH ASSIGNMENT

Technique	Description	Advantages	Disadvantages
Attack aware routing and wave length assignment [37]	Minimizes the damage caused by jamming and achieves significant prevention measures without the need for specialized equipment.	Improves network security and robustness.	Attacking probability varies with respect to the distance from attacking point.
Attack-Aware Wavelength Assignment [38]	Prevention oriented method help attack localization and source identification in the network planning phase.	Minimizes in-band cross talk jamming and number of wavelengths used.	Jamming attack scenarios are not included in the network planning phase.
Maximum Light path Attack Radius [62]	Damage is minimized by routing and wavelength assignment without using any specialized equipment. Set of light paths are arranged.	Improve network security and robustness. Minimum extra cost.	Attack-aware wavelength assignment is not considered.

TABLE III
GAME THEORY APPROACH

Technique	Description	Advantages	Disadvantages
Stochastic anti-jamming game formulation [41]	At each stage of the game, SU observe the spectrum availability, the channel quality, and attacker's strategy from the status of jammed channels.	Achieve better performance than from myopic learning.	Does not work well for ad hoc networks.
Anti-Jamming Channel Hopping Game [44]	Hops across multiple channels. Modeled as a zero-sum anti-jamming game with SU and attackers, both having opposite objectives.	Minimizes worst-case damage caused by attackers.	Learning process goes wrong if SU wrongly estimate the parameters.
To hop or not to hop [46]	Zero-sum game is played between a transceiver pair and a jammer over a parallel fading channel with multiple frequency bands.	Smart jammers are dealt.	Does not deal with Nash equilibrium points.
Game-Theoretical Anti-jamming [51]	The SU proactively hop among accessible channels. The hopping process is formulated as a Markov Decision Process.	Achieve higher payoff than existing approaches. Lower jamming probability.	Signal to Noise ratio is reduced.

C. Game Theory Approach

In these approaches, zero-sum stochastic game is modeled between secondary users SU and attackers. For reliable transmission in cognitive radio networks, multiple channels are reserved for transmitting control messages from time to time according to attacker's strategy. Secondary users are able to avoid the jamming attack by proactively hopping among accessible channels thereby maximizing the payoff function. Different game theory approaches are listed in Table III.

D. Frequency Hopping

In frequency hopping techniques, a transmitter changes the frequency bands on which the signals are transmitted. The entire spectrum of the communication system is divided into a number of frequency bands and the time is divided into time slots. Each user is assigned a frequency-hopping pattern that is served as the spreading code. Frequency hopping techniques are very effective in coping with jamming attacks and different techniques are listed in Table IV.

E. Multi Path Routing

The end-to-end availability provided between the source and the destination for multiple paths is known as multipath availability. An important of multipath routing is to identify a reliable path for data transmission. Multi path routing techniques are listed in Table V.

F. Threshold Based

The reduction of probability of success in the presence of jamming signal can be mitigated by using threshold based schemes. Each node in the network maintains a threshold value and data are transmitted based on the value. Two threshold based schemes are listed in Table VI.

G. Cryptographic Key Distribution

In order to provide security from jamming attack, a well-known task is to provide cryptographic keys to nodes. The most straightforward solution is to encrypt every packet, so that jammers cannot figure out the packet. When the number of nodes is large, the number of keys required will also be large. It is difficult to assign secret keys for all pairs of node.

Open Science Index, Computer and Information Engineering Vol:9, No:2, 2015 publications.waset.org/10003033/pdf

Open Science Index, Computer and Information Engineering Vol:9, No:2, 2015 publications.waset.org/10003033/pdf

One solution is to randomly assign keys and then connect each other with some probability. Different cryptographic key distribution techniques are listed in Table VII.

TABLE IV
FREQUENCY HOPPING

Technique	Description	Advantages	Disadvantages
Code tree based system [23]	A protocol allows a broadcast communication system to dynamically change the spreading codes used by subsets of receivers. The receiver detects jamming by receiving a secondary message without a primary message.	It uses much shorter packets thereby reducing the packet error rate. Spreading codes are dynamically changed.	To mitigate jamming it relies only on keying and not on other physical characteristics.
Time-delayed broadcast [29]	This scheme is used for jamming-resistant broadcast communications in the presence of inside jammers. The broadcast is realized as a series of uni cast transmissions distributed in frequency and time.	Maintain broadcast communications even when multiple nodes are compromised. Network throughput is maximized.	It is designed only for temporarily restoring communications.
MAC-Uncoordinated Frequency Hopping [47]	This scheme uses Media Access Control strategies for collaborative UFH-based broadcast requiring no pre-shared secret keys. Its communication efficiency is improved through node cooperation.	Minimal broadcast delay and reduce the overall energy consumption without pre-shared keys.	Communication efficiency is a bottleneck for practical applications.
Randomized Distributed using frequency hopping [50]	Prevents control-channel jamming as well as identifies compromised nodes through their unique sequences and excludes them from the network.	Each node follows a unique hopping sequence. No extra overhead.	Not applicable for full-duplex communication. Used as a temporary solution for control channel re-establishment.
Anti-jamming Reinforcement ARES [60]	ARES is composed of a rate adaptation and power control modules. Rate adaptation decides between fixed or adaptive-rate assignment. Power control facilitates appropriate clear channel assessment threshold tuning.	Tunes the parameters of rate adaptation and power control. Improve throughput in the presence of jammers.	Utilizes functionalities that are currently unavailable in commercial NIC.
Frequency Hopping anti-jamming [64]	A game theoretic Framework is provided to capture the interactions between a link and a jammer employing FH	Proactive frequency hopping strategy is considered.	FH seems to be inadequate in coping with jamming attacks
Wormhole-Based Anti jamming [68]	Wormholes are used as a defense mechanism using wires, frequency hopping and uncoordinated channel hopping. Mathematical models are developed.	Nodes need not to be synchronized.	Hybrid scheme by combining the three approaches is not considered.
Uncoordinated Spread Spectrum [73]	Enables anti-jamming communication without any secret keys. Randomize the selection of the spreading key such that attackers cannot jam the communication.	Handle an unlimited amount of malicious receivers.	It does not deal with single bit replacement or replacing message parts.
Optimal Uncoordinated Frequency Hopping [75]	The UFH-based anti-jamming communication is a non-stochastic multi-armed bandit problem. It introduced online optimization theory into the frequency hopping strategy design.	The time and space complexity are reduced.	Instead of random frequency hopping, learning first will help to prevent loss.

TABLE V
MULTI PATH ROUTING

Technique	Description	Advantages	Disadvantages
Jamming-aware source routing [57]	Traffic is allocated in multiple-path routing in the presence of jammers.	Achieves optimized throughput.	Effects are characterized statistically and not practically.
Availability History Vectors algorithm based on Multi path Routing [59]	Multiple paths are selected based on the knowledge of paths history. Jamming is addressed at the network level and end-to-end data delivery is restored through multipath routing by improving jamming resilience.	Achieves smaller communication cost and effectively identifies multiple paths. Resistant to variety of jammers.	Wrongly predicts future correlation if the previous path history is not updated correctly.

TABLE VI
THRESHOLD BASED

Technique	Description	Advantages	Disadvantages
Multi-packet transmission (MPT) and Multi-packet reception (MPR)[48]	The effect of jamming signals mitigated based on the probability of success and throughput. Maximum throughput is obtained by the proper adjustment of the transmitting and receiving probability of each node.	Attains maximum throughput.	If either MPT or MPR is used, throughput reduces.
ANTIJAM MAC protocol [31]	It is a simple, fair, and self-stabilizing distributed MAC protocol that is able to make efficient use of a shared communication medium. It mitigates internal and external threats.	Low convergence time and excellent fairness property. Achieves constant throughput at varying network size.	Jammers affecting few bits in a packet cannot be detected.

TABLE VII
CRYPTOGRAPHIC KEY DISTRIBUTION

Technique	Description	Advantages	Disadvantages
Hybrid key pre-distribution [56]	Supports local connectivity and evaluates spatial retreat strategies. Utilizes the properties of random key pre distribution schemes.	Robust key distribution and provides high key connectivity.	Jammer's location cause some un jammed nodes to be disconnected from the network.
Greedy User IDEntification algorithm [66]	Mitigates jamming by identifying compromised users using random assignment of cryptographic keys to hide the location of control channels.	Identifies compromised users without its prior knowledge.	Control messages are not analyzed.

TABLE VIII
HIDING SCHEME

Technique	Description	Advantages	Disadvantages
Packet hiding schemes [27]	Three schemes are developed to combine cryptographic primitives with physical layer attributes, to hide the packets between physical and MAC layers.	Prevents real time packet classification.	Network performance degrades under non congestion when compared to under congestion.
Hiding traffic with camouflage [72]	Min-max approach analyzes the worst-case message delay under jamming. Minimizes delay by increasing redundant traffic into the network.	Decreases message invalidation probability and minimizes delay.	It doesn't improve the performance of nonreactive jamming
Resource-efficient hiding [76]	Prevents the leakage of contextual information by involving in bogus traffic source selection phase and rate assignment phase. Hides information using fake data sources.	Reduces communication overhead. Needs smaller number of fake sources.	Fake sources are static and not dynamic.

H.Hiding Scheme

Hiding schemes are used to hide contextual information's like traffic, data from attackers. It can be hided using fake data source or between layers. Some hiding schemes are listed in Table VIII.

IV. CONCLUSION

The shared nature of wireless network enables the attacker to carry out attacks easily. This paper has surveyed the main aspects of security against jamming attacks, its vulnerabilities, classification of jamming attacks, jamming models and its effective countermeasures. Four different types of jammers involved in PHY jamming have also been discussed. Among the four, reactive jammer at physical layer is found to be the smarter and efficient one. Various jamming prevention techniques are surveyed and its methodology, advantages, and disadvantages are also compared.

ACKNOWLEDGEMENT

This work was supported in part by Anna University recognized research center lab at Francis Xavier Engineering College, Tirunelveli, India.

REFERENCES

[1] G. T. Amariucai, "Physical layer security in wireless networks: Intelligent jamming and eavesdropping", *Ph. D thesis, Louisiana State University, Louisiana*, 2009.

[2] A. D. Wyner, "The wire-tap channel," *The Bell System Technical Journal*, vol. 54, pp. 1355–1387, Oct. 1975.

[3] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," *MobiHoc 05*, pp 46-57, May 2005.

[4] Konstantinos Pelechrinis, Marios Iliofotou and Srikanth V. Krishnamurthy, "Denial of Service Attacks in Wireless Networks: The Case of Jammers", *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp.245-257, April 2011.

[5] M. Acharya and D. Thuente, "Intelligent jamming attacks, counterattacks and (counter)2 attacks in 802.11b wireless networks," *In Proceedings of OPNETWORK Conference*, Aug. 2005.

[6] L. Lazos, S. Liu, and M. Krunz, "Mitigating control-channel jamming attacks in multi-channel ad hoc networks", *In Proceedings of the 2nd ACM conference on wireless network security*, pp.169–180, March 2009.

[7] G. Noubir and G. Lin, "Low-power DoS attacks in data wireless lans and countermeasures" *Mobile Computing and Communications Review*, vol.7, no.3, pp.29–30, July 2003.

[8] Y. Liu, P. Ning, H. Dai, and A. Liu, "Randomized differential DSSS: Jamming-resistant wireless broadcast communication", *IEEE Proceedings of INFOCOM*, pp. 1-9, March 2010.

[9] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: Defenses against wireless denial of service", *In Proceedings of the 3rd ACM workshop on Wireless security*, pp. 80–89, 2004

[10] W. Xu, W. Trappe, and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks," *Proc. First ACM Conf. Wireless Security*, 2008.

[11] Z. Lin and M. V. Schaar, "MAC Layer Jamming Mitigation Using a Game Augmented by Intervention", *EURASIP journal on Wireless Communications and Networking*, pp-1-14, no. 78, 2011.

[12] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defence policies in wireless sensor networks," *In Proceedings of the 26th IEEE International Conference on Computer Communications (INFOCOM '07)*, pp. 1307–1315, May 2007.

[13] B. Awerbuch, A. Richa, and C. Scheideler, "A jamming resistant MAC protocol for single-hop wireless networks," *27th ACM Symposium on Principles of Distributed Computing (PODC '08)*, pp. 45–54, Aug.2008.

[14] U. Patel, T. Biswas, and R. Dutta, "A Routing Approach to Jamming Mitigation in Wireless Multihop Networks", *IEEE Workshop on Local & Metropolitan Area Networks (LANMAN)*, pp. 1-6, Oct. 2011.

[15] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," *In Proceedings of the 1st EuroFGI International Conference on Network Control and Optimization*, pp. 1–12, June 2007.

[16] G. Thamilarasu, S. Mishra and R. Sridhar," Improving Reliability of Jamming Attack Detection in Ad hoc Networks", *International Journal of Communication Networks and Information Security (IJCNIS)*, vol. 3, no. 1, pp. 57-66, April 2011.

[17] D. Chen, J. Deng, and P. K. Varshney, "Protecting wireless networks against a denial of service attack based on virtual jamming," *In MOBICOM -Proceedings of the Ninth Annual International Conference on Mobile Computing and Networking, ACM*, 2003.

[18] D. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in Proceedings of the 25th IEEE Communications Society Military Communications Conference (MILCOM), pp.1075-1081, Oct. 2006.

[19] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attacks and defense strategies," in IEEE Network, pp.41 - 47, May 2006.

[20] Y. Law, P. Hartel, J. D. Hartog, and P. Havinga, "Link-layer jamming attacks on S-Mac," in Proc. 2nd Euro. Wksp. Wireless Sensor Network, pp. 217-225, Feb. 2005.

[21] A. Wood and J. Stankovic, "Denial of service in sensor networks," IEEE Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[22] B. Onings, "PHY and MAC Layer Security in 802.11 Networks", *Ulm University.*

[23] J. T. Chiang, and Y. C. Hu, "Cross-Layer Jamming Detection and Mitigation in Wireless Broadcast Networks", *IEEE/ ACM transactions on networking*, vol.19, no.1, pp. 286-298, Feb. 2011.

[24] H. Yang, H. Luo, F. Ye, S. Lu, and L. Zhang, "Security in mobile ad hoc networks: Challenges and solutions," *IEEE Wireless Communications*, vol. 11, no. 1, pp. 38-47, Feb. 2004.

[25] D. Djenouri, L. Khelladi, and N. Badache, "A survey of security issues in mobile ad hoc and sensor networks", *IEEE communications surveys and Tutorials*, vol. 7, no.4, pp. 2-8, Dec. 2005.

[26] Y. Zhang, and W. Lee, "Security in Mobile Ad-Hoc Networks", *in Book Ad Hoc Networks Technologies and Protocols (Chapter 9), Springer*, 2005.

[27] A. Proano, and L. Lazos, "Packet-hiding methods for preventing selective jamming attacks", *IEEE Transaction Dependable Secure Computing*, vol. 9, No.1, pp. 101–114, Jan 2012.

[28] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel surfing and spatial retreats: defenses against wireless denial of service", *In*

Open Science Index, Computer and Information Engineering Vol:9, No:2, 2015 publications.waset.org/10003033/pdf

Open Science Index, Computer and Information Engineering Vol:9, No:2, 2015 publications.waset.org/10003033/pdf

Proceedings of the 3rd ACM workshop on Wireless security, pp. 80–89, 2004.

[29] S. Liu, L. Lazos, and M. Krunz, "Thwarting Inside Jamming Attacks on Wireless Broadcast Communications", *Proceedings of the fourth ACM conference on Wireless network security WiSec'11*, pp. 29-40, June 2011.

[30] L. Wang, and A. M. Wyglinski, "A Combined Approach for Distinguishing different Types of Jamming Attacks Against Wireless Networks", *IEEE Pacific Rim Conference on Communications, Computers and Signal Processing (PacRim)*, pp. 809–814, Aug. 2011.

[31] A. Richa, C. Scheideler, S. Schmid, and J. Zhang J, "An Efficient and fair MAC protocol robust to reactive interference", *IEEE/ACM Transaction on. Networking*, vol. 21, no. 3, pp.760–771, June 2013.

[32] M. Strasser, B. Danev, and S. Capkun, "Detection of reactive jamming in sensor networks", *ACM Transaction on Sensor Networks*, vol. 7, no. 2, pp.1–29, Aug. 2010.

[33] Y. Xuan, Y. Shen, N. P. Nguyen, and M. T. Thai, "A trigger identification service for defending reactive jammers in WSN", *IEEE Transaction on Mobile Computing*, vol.11, no.5, pp.793–806, March 2012.

[34] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "Reactive jamming in wireless networks: How realistic is the threat?", *In Proceedings of ACM conference on Wireless Network Security*, pp. 47-52, June 2011.

[35] S R Ratna, R Ravi, and B Shekhar, "An Intelligent Approach based on Neuro- Fuzzy Detachment Scheme for Preventing jamming Attack in Wireless Networks", *Journal of Intelligent and fuzzy logic*, Doi 10.3233/IFS-141363, in press, Sep. 2014.

[36] D. Tagra, M. Rahman, and S. Sampalli, "Technique for Preventing DOS Attacks on RFID Systems", *IEEE International Conference on Software, Telecommunications and Computer Networks (SoftCOM)*, pp. 6–10, Sep. 2010.

[37] N. S. Kapo, J. Chen, and L. Wosinska, "A New Approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment", *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, pp. 750-760, June 2010.

[38] M. Furdek, N. S. Kapov, and M. Grbac, "Attack-Aware Wavelength Assignment for Localization of In-band Cross talk Attack Propagation", *Journal of Optical Communication Networking*, vol. 2, no. 11, pp. 1000-1009, Nov. 2010.

[39] F. Ahsan, S. Djahel, F. N. Abdesselam, and S. Mohsin, "Neighbor based Channel Hopping Coordination: Practical against Jammer?", *The 9th IEEE International Workshop on Wireless Local Networks*, pp. 993-998, Oct. 2009.

[40] S. Chen, K. Zeng, and P. Mohapatra, "Jamming-Resistant Communication: Channel Surfing without Negotiation" *IEEE International Conference on Communications*, pp. 1-6, May 2010.

[41] B. Wang, Y. Wu, K. J. R. Liu, and T. C. Clancy, "An Anti-Jamming Stochastic Game for Cognitive Radio Networks", *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 877–889, March 2011.

[42] S. Misra, R. Singh and S.V.R. Mohan, "Geomorphic zonalisation of wireless sensor networks based on prevalent jamming effects", *IET Communication*, vol. 5, no. 12, pp. 1732–1743, Aug. 2011.

[43] Y. Desmedt, R. S. Naini, H. Wang, C. Charnes, and J. Pieprzyk, "Broadcast anti-jamming systems", *In Proc. of the IEEE International Conference on Networks (ICON)*, pp. 349–355, Oct. 1999.

[44] Y. Wu, B. Wang, K. J. R. Liu, and T. C. Clancy, "Anti-Jamming Games in Multi-Channel Cognitive Radio Networks", *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp. 4-15, Jan. 2012.

[45] R. A. Poisel, "Modern Communications Jamming Principles and Techniques", *Artech House Publishers, Second Edition*, 2011.

[46] S. Wei, R. Kannan, V. Chakravarthy, and M. Rangaswamy, "CSI Usage over Parallel Fading Channels under Jamming Attacks: A Game Theory Study", *IEEE Transactions on Communications*, vol. 60, no. 4, pp. 1167-1175, April 2012.

[47] L. Xiao, H. Dai, and P. Ning, "MAC Design of Uncoordinated FH-Based Collaborative Broadcast", *IEEE Wireless Communications Letters*, vol. 1, no. 3, pp. 261-264, June 2012.

[48] J.H. Sarker H.T. Mouftah, "Mitigating the effect of jamming signals in wireless ad hoc and sensor networks", *IET Communications*, vol. 6, no. 3, pp. 311–317, 2012.

[49] C. Popper, M. Strasser, and S. Capkun, "Jamming-resistant broadcast communication without shared keys", *In Proc. of the USENIX Security Symposium*, 2009.

[50] S. Liu, L. Lazos, and M. Krunz, "Thwarting Control-Channel Jamming Attacks from Inside Jammers", *IEEE Transactions on Mobile Computing*, vol. 11, no. 9, pp. 1545-1558, Sep. 2012.

[51] C. Chen, M Song, C. Xin, and J. Backens, "A Game-Theoretical Anti-Jamming Scheme for Cognitive Radio Networks", *IEEE Network*, vol.27, no. 3, pp.22-27, May 2013.

[52] S. Misra, S. K. Dhurandher, A. Rayankula, and D. Agrawal "Using honey nodes for defense against jamming attacks in wireless infrastructure-based networks," *Computers & Electrical Engineering*, vol. 36, pp. 367-382, 2010.

[53] A. Mpitziopoulos, G. Damianos, C. Konstantopoulos, and G. Pantziou, "A survey on jamming attacks and countermeasures in WSNs", *IEEE Surveys & Tutorials on communications*, vol. 11, No. 4, pp. 42-56, 2009.

[54] A. L. Toledo, and X. Wang, "Robust Detection of MAC Layer Denial-of-Service Attacks in CSMA/CA Wireless Networks", *IEEE Transactions on Information Forensics and Security*, vol. 3, no. 3, pp. 347-358, 2008.

[55] S. R. Ratna, and R. Ravi, "Malicious Route Defending Reliable-Data Transmission Scheme for Multi Path Routing in Wireless Network", *World Academy of Science, Engineering and Technology*, vol:8, no:12, pp. 1950-1955, Dec. 2014.

[56] K. Panyim, and P. Krishnamurthy, "A Hybrid Key redistribution Scheme for Sensor Networks Employing Spatial Retreats to Cope with Jamming Attacks", *Mobile Network Application*, vol.10, pp. 715-731, 2009.

[57] P. Tague, S. Nabar, J. Ritcey, and R. Poovendran, "Jamming-Aware Traffic Allocation for Multiple-Path Routing Using Portfolio Selection," IEEE Trans. Networking, vol. 19, no. 1, pp. 184-194, 2011.

[58] Y. Zhang, L. Lazos, and W. Kozma, "AMD: Audit-based Misbehavior Detection in Wireless Ad Hoc Networks", *IEEE Transactions on Mobile Computing*, no. 1, PrePrints PrePrints, doi:10.1109/TMC.2012.257.

[59] H. Mustafa, X. Zhang, Z. Liu, W. Xu, and A. Perrig, "Jamming-Resilient Multipath Routing", *IEEE Transactions on Dependable and Secure Computing*, vol. 9, no. 6, pp. 852- 864, Nov. 2012.

[60] K. Pelechrinis, I. Broustis, S. V. Krishnamurthy, and C. Gkantsidis, "A Measurement-Driven Anti-Jamming System for 802.11 Networks", *IEEE/ACM Transaction on Networking*, vol. 19, no. 4, pp. 1208-1222, Aug. 2011.

[61] P. Tague, M. Li, and R. Poovendran, "Probabilistic mitigation of control channel jamming via random key distribution", *in Proceedings of IEEE PIMRC*, pp.1–5, 2007.

[62] N. S. Kapov, J. Chen, and L. Wosinska, "A New approach to Optical Networks Security: Attack-Aware Routing and Wavelength Assignment", *IEEE/ACM Transactions on Networking*, vol. 18, no. 3, pp.750-760, June 2010.

[63] D. M. Shila, Y. Cheng, and T. Anjali, "Mitigating Selective Forwarding Attacks with a Channel-Aware Approach in WMNs", *IEEE Transactions on Wireless Communications*, vol. 9, no. 5, pp. 1661-1675, May 2010.

[64] K. Pelechrinis, C. Koufogiannakis, and S. V. Krishnamurthy, "On the Efficacy of Frequency Hopping in Coping with Jamming Attacks in 802.11 Networks", *IEEE Transactions on Wireless Communications*, vol. 9, no. 10, pp.3258-3271, Oct. 2010.

[65] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal Jamming Attack Strategies and Network Defense Policies in Wireless Sensor Networks", *IEEE Transactions on Mobile Computing*, vol. 9, no. 8, pp. 1119-1138, Aug. 2010.

[66] P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks", *IEEE Transactions on Mobile Computing*, vol. 8, no. 9, pp.1221-1234, Sep. 2009.

[67] B. Xiao, B. Yu, C. Gao, "CHEMAS: Identify suspect nodes in selective forwarding attacks", *Journal of parallel and distributed computing-Elsevier*, vol. 67, pp.1218–1230, 2007.

[68] M. Cagalj, S. Capkun, and J. P. Hubaux, "Wormhole-Based Anti jamming Techniques in Sensor Networks", *IEEE Transactions on Mobile Computing*, vol. 6, no. 1, pp.100-114, Jan. 2007.

[69] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt, "Spread Spectrum Communications Handbook", *McGraw-Hill*, 2001.

[70] J. Jeung, S. Jeong, and J. Lim, "Anti Jamming – Based Medium Access Control Using Adaptive Rapid Channel Hopping in 802.11: AJ-MAC" *Springer, ICCSA*, pp. 70–82, 2011.

[71] Y. B. Reddy, and S. Srivathsan, "Game Theory Model for Selective Forward Attacks in Wireless Sensor Networks", *IEEE Conference on Control & Automation*, pp.458-463, 2009.

[72] Z. L. Wenye, and W. C. Wang, "Hiding Traffic with Camouflage: Minimizing Message Delay in the Smart Grid under Jamming", *IEEE international conference on computer communications*, pp. 3066-3070, 2012.
[73] C. Popper, M. Strasser, and S. Capkun, "Anti-Jamming Broadcast Communication using Uncoordinated Spread Spectrum Techniques", *IEEE Journal on Selected Areas in Communications*, vol. 28, no. 5, pp.703-715, June 2010.
[74] W. Saad, X. Zhou, B. Maham, T. Basar, and H. V. Poor, "Tree Formation with Physical Layer Security Considerations in Wireless Multi-Hop Networks, *IEEE Transactions on Wireless Communications*, vol. 11, no. 11, pp.3980-3991, Nov. 2012
[75] Q. Wang, P. Xu, K. Ren, and X. Y. Li, "Towards Optimal Adaptive UFH-Based Anti-Jamming Wireless Communication", *IEEE Journal on Selected Areas in Communications*, vol. 30, no. 1, pp.16-30, Jan. 2012.
[76] A. Proano, and L. Lazos, "Hiding Contextual Information in WSNs", *IEEE International Symposium on a World of Wireless, Mobile and Multimedia Networks*, pp. 1-6, 2012
[77] B. Sklar, Digital Communications, Fundamentals, and Applications. *Prentice-Hall*, 2001.
[78] A. Proano, and L. Lazos, "Perfect Contextual Information Privacy in WSNs under Colluding Eavesdroppers", *WiSec'13 Proceedings of the sixth ACM conference on Security and privacy in wireless and mobile networks*, pp.89-94, 2013.
[79] J. T. Chiang, and Y.C. Hu, "Dynamic jamming mitigation for wireless broadcast networks", *In proceedings. Of INFOCOM*, pp. 1211–1219, 2008.

S. Raja Ratna received her B.E degree in Electrical and Electronics Engineering from The Indian Engineering College, Tirunelveli in 2000, and the M. Tech degree in Computer and Information Technology from Manonmanium Sundaranar University, Tirunelveli in 2005. She is working towards Ph. D degree at the Information and Communication Engineering at Anna University, Chennai. Her research interests include denial-of-service attacks, jamming attacks, secure routing algorithm and security in networks.

Dr. R. Ravi is an Editor in International Journal of Security and its Applications (South Korea). He is presently working as a Professor & Head and Research Centre Head, Department of Computer Science and Engineering, Francis Xavier Engineering College, Tirunelveli. He completed his B.E in Computer Science and Engineering from Thiagarajar College of engineering, Madurai in the year 1994 and M.E in Computer Science and Engineering from Jadavpur Government research University, Kolkatta. He has completed his Ph. D in Networks from Anna University Chennai. He has 19 years of experience in teaching as Professor and Head of department in various colleges. He published 25 International Journals. He is also a full time recognized guide for various Universities. Currently he is guiding 18 research scholars. His areas of interest are Virtual Private networks, Networks, Natural Language Processing and Cyber security.

Open Science Index, Computer and Information Engineering Vol:9, No:2, 2015 publications.waset.org/10003033/pdf