On Classifying and Evaluating the Effect of Jamming Attacks

Yu-seung Kim, Heejo Lee
Division of Computer & Communication Engineering
Korea University, Seoul, Republic of Korea
Email:{corekey,heejo}@korea.ac.kr

***Abstract*—While various wireless networks have advanced rapidly and become an indispensable infrastructure in our network environment, jamming attacks are the common challenging problem that makes them unavailable. Jamming attack is easy to be launched with little efforts while its damage is severe since it disrupts the communication of all the nodes in the jamming range. In this paper, we expand the definition of traditional jamming in order to cover more attacks like link-layer jamming and propose taxonomies of jamming attacks and countermeasures in wireless networks. We also propose the generalized risk criteria to evaluate the effect of jamming and instantiate an application through case study. By providing a classification of jamming attacks and an evaluation of their effect, we expect to reveal the undeveloped area of related works and to foster studies on them.**

I. Introduction

Even though various wireless networks, such as WPAN, WLAN, WMAN, and WWAN, become the essential infrastructure in our life, they are well known to be more vulnerable than the wired network since they communicate over the shared medium to which attackers are easily accessible. There have been related works which deal with the various threats over the wireless networks. The author in [1] introduces seven attacks to wireless networks and their countermeasures. Those attacks aim at confidentiality and integrity, not availability. In [2], the author presented the taxonomy of DoS attack on wireless sensor networks.

Generally, the attacks against availability intend to be realized with less effort as compared with those against confidentiality and integrity. *Jamming* is the one of such availability attacks which can be easily carried out. It is defined as the intended transmission of radio signals that disrupt legitimate communications by decreasing the signal to noise ratio. Historically, jamming has been a critical issue for a long time in the military field because it is used for neutralizing adversary's wireless communication system and it should be defeated to protect friendly forces'. Spread spectrum technologies such as frequency hopping spread spectrum (FHSS) and direct-sequence spread spectrum (DSSS) have been used as a countermeasure against jamming attacks. However, it is well known that it is not suitable to be adopted by commercial wireless devices due to high implementation costs and performance degradation caused by spreading techniques. Moreover, particular types of attack such as broadband noise jamming [3] still can influence on the devices which are equipped with spreading techniques. These facts show that jamming is easy to attack but hard to defend.

Recently, some works revealed that jamming attacks are feasible in the widely deployed wireless networks and warned their dangerousness [4]–[6]. They show that certain type of jamming aims at the link layer of the victim node and interrupt the communication with less efforts than the jammer directly attacking the physical layer. In this paper, thus, we expand the traditional concept of jamming with a broader viewpoint. We present the definition of jamming as follows.

"Jamming is one sort of denial-of-service attacks in the wireless communication, which disturbs the operation of physical or link layers in legitimate nodes by transferring illegitimate signals."

This definition includes not only the traditional jamming, but virtual jamming such as spurious RTS/CTS attack and NAV attack on the IEEE 802.11 MAC protocol which is introduced in [7]. On the other hand, the well-known TCP SYN flooding is not included in this coverage even when it is launched over wireless networks. It is the denial-of-service attack against transport layer, not physical or link layer. In short, the denial-of-service attacks which target from network layer to application layer is not regarded as the domain of jamming in this paper.

Through the multifarious jamming-related papers, we found that the concept of jamming is used on various wireless networks and it is difficult for a novice to get an entire map and to catch up the currency of this field. Pelechrinis et al. in [8] provide the survey of jamming both in the physical layer and link layer. They focus on introducing the detailed algorithms in related works rather than classifying them according to consistent criteria. Xu et al. make a notable contribution on jamming studies in wireless sensor networks, wireless ad-hoc network, and WLAN [5], [9], [10]. They define four types of jamming attacks and propose various detecting and mitigating mechanisms to cope with them. The authors in [4], [7], [11] define jamming attacks in WLAN and also provide the solutions to detect and to prevent them. Husso in [12] analyzes the effect of physical-layer jamming in IEEE 802.16 WiMAX system. Kim et al. in [13] introduce a link-layer jamming in IEEE 802.16 WiMAX system.

In this paper, we propose systematic taxonomy and evaluation method of jamming attacks on wireless networks in order to make following contributions in this field.

- Providing the holistic map of jamming and its defense technologies
- Developing the metrics which can evaluate the harmful

effect from jamming attack
- Fostering studies on the unknown area of jamming technologies by categorizing both the realized and the possible jamming attacks

Our classification methods will be useful not only to the beginners for research in this area, but also to the network administrators who seek practical approaches to make their wireless networks to be more resistant to jamming attacks. In addition, the evaluation methods can be used to measure the effectiveness of new defense mechanisms against jamming attacks.

After introduction, Section II-B discuss the risk criteria of jamming attacks. Due to the page limit, we provide the taxonomy of jamming attacks, detection methods, and mitigation methods as the separated appendices. To exemplify the application of the proposed risk criteria and taxonomies to the existing jamming attacks, a case study on the WLAN is provided in Section III. And we conclude the paper in Section IV.

II. Risk Criteria of Jamming Attacks

Before starting to describe the jamming attacks, it is necessary to set up the risk criteria to evaluate the risk of each jamming. Well-refined metrics are essential to quantify the noxious effect, which need to be generalized to cover most jamming attacks. First, we classify the metrics presented in the related studies and then we develop the reconstructed metrics to be used in general situations.

A. Evaluation Category of Jamming Effect

We categorize all the risk criteria into five different types in Fig. 1.

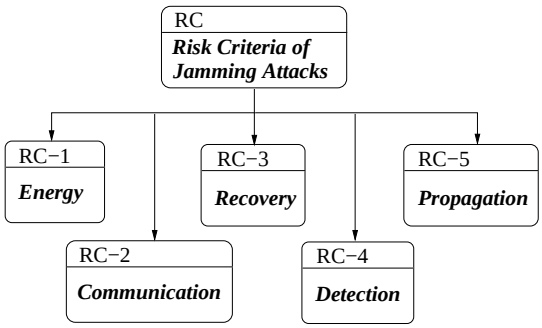

Fig. 1. Risk Criteria of Jamming Attacks

[RC-1] Energy

In wireless networks, jammers try to consume less energy since it is the constrained resource. Especially, the longevity of node is an important factor in wireless sensor networks, thus both jammers and legitimate nodes shall compete to exist longer than their opponents by more efficient strategy of saving energy consumption. The jamming attack which spends less energy is more effective if the legitimate node do not have the unlimited energy resources. *Jamming Defense Power Efficiency (JDPE)* in [14] is one of the metric which represents the energy efficiency of jamming attack. It is defined as $JDPE = P_A/P_D$, where P_A is the power consumption by attacker, and P_D is the power consumption by defender. It implies that the jammer exists longer than the legitimate nodes if their energy capacity is equal and $JDPE > 1$.

[RC-2] Communication

The more harmful a jamming attack is, the more data would be lost during the communication. In the station-based viewpoint, *Packet Send Ratio (PSR)* and *Packet Delivery Ratio (PDR)* can be used to compare jamming effects on communication [5], [10]. PSR is defined as $PSR = m/n$, where n is the number of packets intended to be sent and m is the number of packets sent successfully. While PSR is measured only in the transceiver, PDR is measured in both the transceiver and the receiver. PDR in the receiver is measured by counting the number of packets passing MAC layer without errors and PDR in the transceiver is measured by counting the number of acknowledgements from the receiver. It is defined as $PDR = m/n$, where n is the number of packets sent from transceiver and m is the number of successfully received packets in the receiver.

While PSR and PDR are measured in link layer, *Signal-to-Noise Ratio (SNR)* [15] and *Bit Error Rate (BER)* [16] are the metrics which can be obtained in physical layer. These metrics are more suitable to represent the effect of physical jamming.

In the network-based viewpoint, we can intuitively define the ratio of jammed region to total network area, $JAR = A_J/A_T$, where A_J is the size of jamming region and A_T is the size of total network region. These can be substituted by the number of jammed nodes and the number of total nodes, respectively. However, JAR has the problem, which is hard to suitably express network partitioning by jamming. Even when the number of jammed nodes is equal, a partitioned network affected by jamming is thought as damaged more severely than the non-partitioned one. *Connectivity Index* [8], [17] is able to well explain this comparison. It is defined as $CI = E/V^2$, where E is the number of unjammed directional link between nodes and V is the total number of nodes in the network. CI is especially useful in the network on which the connectivity is important, such as wireless ad-hoc network.

[RC-3] Recovery

Most of wireless networks adopts the forward error correction such as *Reed-Solomon coding* and *turbo coding*. Transceivers normally send the additional bits to be used for recovering the original data in receivers when the transferred data are corrupted. However, the receiver shall fail to recover the original data when a jamming attack is intense.

On the other hand, the recovery in the aspect of network can be considered with different strategies. For instance, routing algorithms recover the routing path from damaged nodes in wireless sensor networks. More harmful jammer tries to attack cluster heads or base-stations than leaf nodes to make the network hard to recover.

[RC-4] Detection

If a jammer transmits the signal in the way similar to a

legitimate node, it will be hard to be detected. Or the jammer which transmits the signal only while the legitimate node transmits is harder to be detected than the jammer which transmits the signal continuously. It is considered that this type of jammer has the stealth property. Naturally, the jamming attack which lowers the probability of detection is classified as more harmful jamming attack.

[RC-5] Propagation

Some type of jamming attacks proliferate the damaged area into their neighborhood. *Spurious RTS/CTS attack* introduced in [7] falsely blocks the normal communication by sending spurious RTS/CTS frames in IEEE 802.11 MAC protocol. The misbehaving frames sent by jammer affect the neighboring outer nodes as well as the nodes in its transmitting range. The propagation effect of a jammer is simply defined by $PE = A_P/(A_I \cdot t)$, where A_P is the size of entire damaged area or the number of damaged nodes after t units of time passes and A_I is the size of the initial jamming range or the number of initially damaged nodes.

B. Unified Metrics for Evaluating Risk of Jamming

It is not easy to define a single metric with five types of risk criteria because the portion of each risk criterion to the all quite varies in the given network environments. For example, most of sensor networks operating at low speed take a serious view of energy since each sensor node should sustain for a long period with the limited battery life. On the other hand, WLAN devices indoor normally are plugged, and thus they are more interested in communication rather than energy. Therefore, we express various aspects of jamming effects with a tuple for convenience in comparing jamming attacks. If the jamming effects from two jamming attacks, $J1$ and $J2$, are measured respectively as $JE_{J1} = (a_1, b_1)$ and $JE_{J2} = (a_2, b_2)$, where $a_1 > a_2$, $b_1 < b_2$, it means that the jamming effect of $J1$ is bigger than the other on the first element and the jamming effect of $J2$ is bigger than the other on the second element .

In terms of a station, the jamming effect is expressed as following 3-tuple with the metrics in *RC-1 (Energy)*, *RC-2 (Communication)*, and *RC-3 (Recovery)*.

$$JE_{sta}(t) = \left(\frac{E_S(t)}{\sum_k E_{J,k}(t)}, \frac{\sum_k P_{L,k}(t)}{\sum_k P_{T,k}(t)}, \frac{F_L(t)}{F_F(t)} \right), \qquad (1)$$

where JE_{sta} is the accumulated jamming effect on a given station during t units of time, E_S is the energy spent in a station during t, $E_{J,k}$ represents the energy spent in the k_{th} jammer during t, $P_{T,k}$ represents the number of packets intended to transmit in the k_{th} transceiver during t, $P_{L,k}$ is the number of packets, which are sent from k_{th} transceiver but not received by jammers in a station during t, F_F is the number of received frames failed to reassemble in a station during t, and F_L is the number of frames still not recovered even by forward error correction algorithms or retransmission among F_F frames during t.

On the other hand, the effect of jamming in terms of a network is expressed as following 5-tuple by integrating *RC-1 (Energy)*, *RC-2 (Communication)*, *RC-3 (Recovery)*, *RC-4 (Detection)*, and *RC-5 (Propagation)*.

$$JE_{net}(t) = \left(\frac{E_N(t)}{\sum_k E_{J,k}(t)}, \frac{C_A(t)}{C_T}, \frac{N_L(t)}{N_F(t)}, T_D, \frac{A_E(t)}{A_S} \right), \qquad (2)$$

where JE_{net} is the accumulated jamming effect on a given network during t units of time, E_N is the energy spent in a network during t, E_J is the energy spent in a jammer during t, C_T is the total number of connections in a network, C_A is the number of connections affected by jammers after t, N_F is the number of nodes affected by jammer during t, N_L is the number of nodes not recovered even by recovery strategies among N_F during t, T_D is the minimum time spent to detect the jammer in a network, A_S is the size of area or number of nodes in jamming region in the starting point of observation, and A_E is the size of area or number of nodes in jamming region expanded after t. The second element uses the number of connections instead of the number of nodes since it expresses the jamming effect much more accurately. But, the number of nodes is used in the third element since we assume that the individual recovery of connections does not occur separately in a general node.

III. Case Study: Evaluation of Jamming Attacks

In order to show the validity of our risk criteria and taxonomies and to instantiate the proposed mechanism, we evaluate the effect of virtual jamming attacks. As we mentioned in Appendix A, there are many types of jamming attacks on various wireless networks. In this case study, however, we implement jamming attacks only on WLAN for the distinct comparison of them. The labels for jamming attacks and their countermeasures are referred in the appendices.

A. Test Setup

We use three laptops equipped with CISCO Aironet CB21AG WLAN device based on Atheros 5212 chip-set. The WLAN devices are operated on MadWifi-v0.9.4 driver [18] with Linux 2.6.24 kernel. Each laptop acts as an access-point (AP), a legitimate station and a jammer, respectively. The jammer uses modified MadWifi driver [19], which disables carrier-sense, virtual carrier sense and post-frame backoff, made by Anderson et al. The AP and the station communicate with each other over the channel 12 (2.467GHz) of IEEE 802.11g in the same room. Using iperf-v2.0.4 [20], the AP transmits 1Mbps UDP traffic to the station. The jammer is installed in next door and tries to interrupt the communication between the AP and the station while changing its type of jamming. In this experiment, we use Eq. (1) to compare the effect of jamming attacks in terms of a legitimate node. For each jamming, we measure the energy consumption of battery in each laptop and the packet loss from the UDP traffic. Any recovery features and statistics for retransmission are not provided by the given driver, so the jamming effect on recovery cannot be measured.

The transmission power of the AP and the station is set to 0dBm (1mW), and the first jammer makes a connection

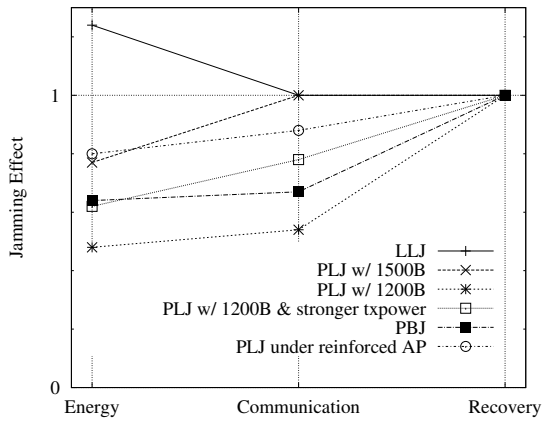

Fig. 2. Comparison of the Effect of Various Jammers (LLJ:Link-layer Jammer, PLJ:Physical-layer Jammer, PBJ:Partial-band Jammer)

with the AP and broadcasts 1500 bytes of ping packets (up to 1Mbps) to the network with 0dBm of transmission power. This assumes that the jammer knows well about the network and is able to connect to the network as legitimate nodes are. Since the jammer ignores the carrier-sense and skips the back-off operation, the whole nodes in the network are affected by the broadcasted frames. It makes the link layer of the legitimate node be blocked to send any data. Thus, this jammer is categorized as *link-layer Jamming (JA-2-1-2)*. The second jammer acts as an independent AP using same frequency channel with the AP. Except for not associating with the AP, all the other configurations are identical to the first jammer. The frames from this jammer are considered as noise and are dropped in the physical layer of the legitimate node. Thus it belongs to *noise Jamming (JA-1-1-1)* and *physical-layer Jamming (JA-2-1-1)*. It is also *pulse Jamming (JA-1-2-2)* since it periodically transmits a packet and pauses for a short while without back-off. The third jammer is only different with the second jammer in that it broadcasts the smaller size of ping packets (1200 bytes). The fourth jammer increases the transmission power of the third jammer into 18dBm (63mW). The second, the third, and the fourth jammer are *full-band noise jamming* since the bandwidth of jamming frequency is equal to one of legitimate nodes. To implement the *partial-band noise jamming*, we have the fifth jammer use the channel 9. Because the bandwidth of the channel 9 (2.441GHz - 2.463GHz) overlaps the half of the bandwidth of the channel 12 (2.456GHz - 2.478GHz). All the other configurations are same with the fourth jammer. Lastly, in order to show the effect of mitigation mechanisms on jamming attacks, we simply adopt the *reinforcement (JM-1-1-1)* to the second jammer. The AP increases the transmission power to 18dBm (63mW), while others remain 0dBm (1mW).

B. Test Results

In Fig. 2, the jamming effects on six different cases are plotted on the parallel coordinate system. Note that the recovery mechanisms and the statistics for retransmission are not provided in this experiment and thus we simply set the jamming effects on recovery to 1. The energy consumption of the station is almost consistent, while the energy consumption of the AP varies for each case. As shown in Fig. 2, the link-layer jammer marks the highest jamming effect in all area. The physical-layer jammer relatively marks the lower jamming efficiency than the link-layer jammer. Even though two jammers send the same amount of packets and consume the same amount of energy, the link-layer jammer causes the AP to spend more energy on receiving malicious packets. The third jammer, which sends the smaller size of packets, shows the lowest jamming efficiency by and large. The fourth jammer, which increases the transmission power, and the fifth jammer, which is a partial-band noise jammer, mark the better jamming effect than the third jammer. The fifth jammer shows the lower jamming efficiency on communication than the fourth jammer. Lastly, the second jammer under the higher-powered AP increases the jamming effect on energy a bit, but decreases the jamming effect on communication.

We summarize the test results as follows.

- The link-layer jamming interfere the victim network more effectively than the physical-layer jamming in the aspect of energy.
- As a jammer knows more detail information about the victim network (e.g. how to join and which channel it uses), the effect of attack will be more effective and efficient.
- The active defense mechanism like *reinforcement* decreases the jamming effect on communication, but increases it on energy in return.

IV. Conclusion

In this paper, we newly define the term "*jamming*" and provide a taxonomy of jamming attacks in wireless networks. We re-classify the existing risk criteria and present unified metrics to fairly compare the effect of various jamming attacks. Detecting and mitigating methods of jamming which are recently proposed in related studies are categorized according to the separate classification criteria. From the presented taxonomies and the case study using them, we reveal that which sort of jammer is more harmful in a given environment. Moreover, there are no common effective and efficient methods to detect and mitigate jamming attacks, yet. It varies on the property of jamming.

By presenting our work, we expect that it will be used as the map of studies related to jamming and it will provide the holistic view for research groups and fields. It also reveals the area with which is not deal in the existing studies and boost a series of new studies. For example, there have been lots of studies on jamming in WLAN and wireless sensor networks, both of which are based on CSMA/CA. Recently, emerging technologies, such as Mobile WiMAX using OFDM, are actively deployed in some countries, thus more jamming studies on these technologies are required. The countermeasures to mobile jammers also need to be developed as the mobile stations have larger bandwidth and stronger computing power than before. And we expect that the proposed risk criteria would be used to evaluate the effect of upcoming jamming

attacks as well as existing jamming attacks. Of course, the proposed taxonomies should be reorganized and expanded with the advent of new jamming attack. Even so it will be used for the starting point of works to fight with them.

ACKNOWLEDGMENT

This research was supported by the MKE(Ministry of Knowledge Economy), Korea, under the ITRC(Information Technology Research Center) support program supervised by the NIPA(National IT Industry Promotion Agency)(NIPA-2009-(C1090-0902-0016)). Additionally, this research was supported by Korea SW Industry Promotion Agency (KIPA) under the program of Software Engineering Technologies Development and Experts Education.

REFERENCES

[1] D. Welch and S. Lathrop, "Wireless security threat taxonomy," in *Information Assurance Workshop*, 2003.

[2] A. D. Wood and J. A. Stankovic, *Handbook of Sensor Networks: Compact Wireless and Wired Sensing Systems*. CRC Press, 2004, ch. A Taxonomy for Denial-of-Service Attacks in Wireless Sensor Networks.

[3] R. A. Poisel, *Modern Communications Jamming Principles and Techniques*. Artech House, Inc., 2004, ch. 2.

[4] J. Bellardo and S. Savage, "802.11 denial-of-service attacks: Real vulnerabilities and pratical solutions," in *12th USENIX Security Symposium*, 2003.

[5] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks," in *the 6th ACM international symposium on Mobile ad hoc networking and computing*, 2005.

[6] A. Wood, J. Stankovic, and G. Zhou, "Deejam: Defeating energy-efficient jamming in ieee 802.15.4-based wireless networks," in *Sensor, Mesh and Ad Hoc Communications and Networks*, 2007.

[7] D. Chen, J. Deng, and P. K. Varshney, "Protecting wireless networks against a denial of service attack based on virtual jamming," in *Poster Session of MobiCom*, 2003.

[8] K. Pelechrinis and M. Iliofotou, "Denial of service attacks in wireless networks: The case of jammers," unpublished. [Online]. Available: http://www.cs.ucr.edu/~kpele/Jamming.pdf

[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 (WiSe '04)*, 2004.

[10] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies," *IEEE Network*, 2006.

[11] D. J. Thuente and M. Acharya, "Intelligent jamming in wireless networks with applications to 802.11b and other networks," in *Proc. MILCOM*, 2006.

[12] M. J. Husso, "Performance analysis of a wimax system under jamming," Master's thesis, Helsinki University of Technology, 2006.

[13] Y. Kim, H.-K. Lim, and S. Bahk, "Shared authentication information for preventing ddos attacks in mobile wimax networks," in *Consumer Communications and Networking Conference*, 2008.

[14] S. Khattab, D. Mossé, and R. Melhem, "Honeybees: Combining replication and evasion for mitigating basestation jamming in sensor networks," in *Parallel and Distributed Processing Symposium*, 2006.

[15] D. Schleher, *Electronic Warfare in the Information Age*. Artech House, Inc., 1999.

[16] A. Vlavianos, L. K. Law, I. Broustis, S. V. Krishnamurthy, and M. Faloutsos, "Assessing link quality in ieee 802.11 wireless networks: Which is the right metric?" in *IEEE 19th International Symposium on Personal, Indoor and Mobile Radio Communications*, 2008.

[17] G. Noubir, "On connectivity in ad hoc networks under jamming using directional antennas and mobility," in *Wired/Wireless Internet Communications*, 2004.

[18] (2008, Feb.) Madwifi v0.9.4. The MadWifi project team. [Online]. Available: http://madwifi-project.org/

[19] E. Anderson, G. Yee, C. Phillips, D. Sicker, and D. Grunwald, "Commodity ar52xx-based wireless adapters as a research platform," University of Colorado at Boulder, Department of Computer Science, Campus Box 430, Technical Report CU-CS-XXXX-08, April 2008.

[20] (2008, Mar.) Iperf v2.0.3. NLANR/DAST. [Online]. Available: http://sourceforge.net/projects/iperf

[21] V. Gupta, S. Krishnamurthy, and M. Faloutsos, "Denial of service attacks at the mac layer in wireless ad hoc networks," in *MILCOM*, 2002.

[22] W. Chen, D. Chen, G. Sun, and Y. Zhang, "Defending against jamming attacks in wireless local area networks," in *Autonomic and Trusted Computing*, 2007.

[23] Y. Law, L. van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energy-efficient link-layer jamming attacks against wireless sensor network mac protocols," in *the 3rd ACR workshop on Security of ad hoc and sensor networks*, 2005.

[24] K. Ma, Y. Zhang, and W. Trappe, "Mobile network management and robust spatial retreats via network dynamics," in *Resource Provisioning and Management in Sensor Networks*, 2005.

[25] C. Won, J.-H. Youn, , and H. Ali, "Impact of high-mobility radio jamming in large-scale wireless sensor networks," in *Emerging Directions in Embedded and Ubiquitous Computing*, 2006.

[26] H. Sun, S. Hsu, and C. Chen, "Mobile jamming attack and its countermeasure in wireless sensor networks," in *Advanced Information Networking and Applications Workshops*, 2007.

[27] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," in *Proceedings of the first ACM conference on Wireless network security (WiSec '08)*, 2008.

[28] G. Thamilarasu, S. Mishra, and R. Sridhar, "A cross-layer approach to detect jamming attacks in wireless ad hoc networks," in *Military Communications Conference*, 2006.

[29] W. Xu, "On adjusting power to defend wireless networks from jamming," in *4th Annual International Conference on Mobile and Ubiquitous Systems : Networking & Services*, 2007.

[30] A. Mpitziopoulos, D. Gavalas, and G. P. C. Konstantopoulos, "Defending wireless sensor networks from jamming attacks," in *Personal, Indoor and Mobile Radio Communications*, 2007.

[31] J. Chiang and Y. Hu, "Cross-layer jamming detection and mitigation in wireless broadcast networks," in *International Conference on Mobile Computing and Networking*, 2007.

[32] ——, "Dynamic jamming mitigation for wireless broadcast networks," in *INFOCOM*, 2008.

[33] M. Strasser, S. Capkun, C. Popper, and M. Cagalj, "Jamming-resistant key establishment using uncoordinated frequency hopping," in *IEEE Security and Privacy*, 2008.

[34] D. Slater, P. Tague, R. Poovendran, and B. J. Matt, "A coding-theoretic approach for efficient message verification over insecure channels," in *Proc. of the Second ACM Conference on Wireless Network Security (WiSec'09)*, 2009.

[35] W. Xu, W. Trappe, and Y. Zhang, "Channel surfing: Defending wireless sensor networks from interference," in *Information Processing In Sensor Networks*, 2007.

[36] A. D. Wood, J. A. Stankovic, and S. H. Son, "Jam: a jammed-area mapping service for sensor networks," in *24th IEEE Real-Time Systems Symposium*, 2003.

[37] E. Altman, K. Avrachenkov, and A. Garnaev, "A jamming game in wireless networks with transmission cost," in *First EuroFGI International Conference, NET-COOP*, 2007.

[38] M. Li, I. Koutsopoulos, and R. Poovendran, "Optimal jamming attacks and network defense policies in wireless sensor networks," in *INFOCOM*, 2007.

[39] T. X. Brown, J. E. James, and A. Sethi, "Jamming and sensing of encrypted wireless ad hoc networks," in *Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing*, 2006.

[40] P. Codenotti, A. Sprintson, and J. Bruck, "Anti-jamming schedules for wireless broadcast systems," in *ETR070, California Institute of Technology*, 2005.

[41] B. Makarevitch, "Jamming resistant architecture for wimax mesh network," in *Military Communications Conference*, 2006.

[42] M. Cagalj, S. Capkun, and J. Hubaux, "Wormhole-based anti-jamming techniques in sensor networks," *IEEE Trans. Mobile Comput.*, vol. 6, no. 1, pp. 100–114, Jan. 2007.

[43] G. Alnifie and R. Simon, "A multi-channel defense against jamming attacks in wireless sensor networks," in *International Workshop on Modeling Analysis and Simulation of Wireless and Mobile Systems*, 2007.

APPENDIX A
CATEGORY OF JAMMING ATTACKS

There are two principles when we classify the jamming attacks: 1) It must include the jamming attacks introduced in the recently proposed studies exhaustively. 2) The classification criterion should be general, not be dependent on the specific wireless networks. With these principles, we collect the related studies about jamming attacks and re-classify them. Similar attacks are merged into one category and some items are newly added into the category. Fig. 3 is the category devised under these conditions.

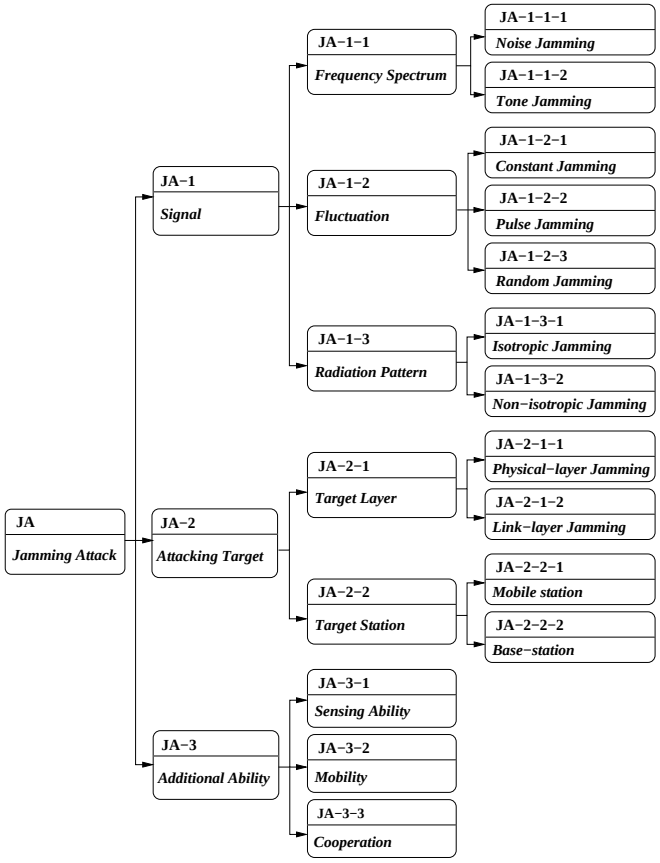

Fig. 3. Category of Jamming Attacks

[JA-1] Signal

With the three different sorts of aspects concerned with signal, jamming attacks can be categorized as follows.

[JA-1-1] Frequency Spectrum

When the jamming signal is represented in the frequency domain, it is divided into *noise jamming (JA-1-1-1)* and *tone jamming (JA-1-1-2)*. *Noise jamming* has the bandwidth of signal over the frequency spectrum, while tone jamming attacks only the meaningful tones in the frequency spectrum. *Noise jamming (JA-1-1-1)* is again divided into *barrage jamming (or full-band jamming)* and *spot jamming (or partial-band jamming)*. The former bandwidth of jamming frequency is wider than or equal to the bandwidth of victim's system. The latter is the other case. *Tone jamming (JA-1-1-2)* is the energy-saving strategy to attack only the critical frequency in the victim's system, such as pilot sub-carrier in the WiMAX system. It is divided into *single-tone jamming* and *multiple-tone jamming* according to the number of tones on which it targets.

[JA-1-2] Fluctuation

The operation of jamming attacks can be fluctuated as time passes by. For instance, a jammer fluctuates between the period of transmitting signal and the period of sleeping to minimize the energy consumption instead of transmitting signal constantly. *Pulse jamming (JA-1-2-2)* fixes the duration of transmitting phase and sleeping phase, while the *random jamming (JA-1-2-3)* does not fix them.

[JA-1-3] Radiation Pattern

According to radiation pattern of jamming signal, jamming attacks can be divided into *isotropic jamming (JA-1-3-1)* and *non-isotropic jamming (JA-1-3-2)*. The *isotropic jamming* uses the omni-directional antenna, thus the radiation pattern of signal is close to a circle in 2D. Relatively, the non-isotropic jamming uses the directional antenna, and radiates the more signals into the intended area with same energy. Therefore, non-isotropic jamming is more effective and efficient when the attacker knows the exact location of target nodes.

[JA-2] Attacking Target

Jamming attacks are classified by the target which it aims at. In this category, target layer and target station can be considered, respectively.

[JA-2-1] Target Layer

From the definition of jamming in this paper, it targets physical layer (JA-2-1-1) or link layer (JA-2-1-2). Most traditional jamming attacks aim at preventing the physical layer of receiver from analyzing signal, reassembling it and passing it to the link layer. On the other hand, *link-layer jamming* causes victim nodes to malfunction by using vulnerabilities in link layer. This is known as more effective jamming attack than the traditional jamming because it can succeed to damage victims by transmitting only small number of illegitimate frames. The link layer jamming attacks which are feasible in IEEE 802.11 MAC are introduced in [4] [7] [11] [21] [22]. In [23], the authors present the link layer jamming over S-MAC, LMAC, and B-MAC of wireless sensor networks. The jamming attacks in IEEE 802.16e-2005 (Mobile WiMAX) are also presented in [13]. Because most of them have the propagation property, *RC-5* is the useful risk criterion to measure the damage of jamming.

[JA-2-2] Target Station

The jamming attacks can be classified according to the role of targeting element in the wireless networks. In the network, which does not have base-stations or in which the role of base-station is not critical, such as wireless ad-hoc network, attacking base-stations is not so powerful. However, WMAN or WWAN such as Mobile WiMAX largely depend on base-stations in operating the network. When a jammer only attacks

a base-station, all the nodes in the range of the base station will not work properly any more. *Base-station jamming (JA-2-2-2)* is more destructive than *mobile station jamming (JA-2-2-1)* in this networks.

[JA-3] Additional Ability

Some types of jammer strengthen its effect by additional abilities.

[JA-3-1] Sensing Ability

In famous *Sun Tzu's Art of War*, there is a saying,

"If you know yourself and your enemy you win hundred battles out of a hundred."

A jammer can sense the packets sent from victim's devices to attack more effectively by knowing the victim's information. The *reactive jammer* represented in [5] [10] has this sensing ability. When wireless channels are not used by any nodes, this jammer does not transmit any signal. It starts to send the signal when it senses any signal from the wireless channel. Due to this reason, it is more difficult to detect this jammer than non-sensing jammer. In the general environments, sensing jamming attacks consume more energy, damage the victim's communication more severely and are more difficult to be detected than non-sensing jamming attacks.

[JA-3-2] Mobility

If a jammer is mobile, it will be more difficult to detect it in spite of more energy consumption. When it is detected, it may already leave the position and disrupt nodes in another position. It also degrades the performance of re-routing algorithms. Additionally, It is possible to partition the given network as shown in [24]. In [25] [26], authors model the mobile jamming in wireless sensor networks and show that it severely degrades the performance of routing algorithms and effectively attacks the networks by finding critical paths. In sum, mobile jamming has clear benefits against stationary jamming on the aspect of communication, recovery, detection and propagation despite of moving costs.

[JA-3-3] Cooperation

When multiple jammers are deployed in the field, they can cooperate together or cannot. The cooperated jammers may communicate with each other during attack, or may be synchronized in advance. In case jammers are able to communicate with each other during attack, it adapts to the dynamically changing network environments even though the probability of being detected by signaling messages between jammers will be increased. The synchronized jammers before attack will be vice versa. In [14], the author presents the similar idea by defining four different type of jamming attack, (un)synchronized-(un)coordinate attacks.

APPENDIX B
DETECTING THE JAMMING ATTACKS

To classify the jamming detection algorithms, we introduce another classification criteria from those used in the category of jamming attacks, since they are not quite match with the detecting methods. Fig. 4 shows the category of jamming detection algorithms with three classification criteria, *intra-node approach*, *intra-network approach*, and *inter-node approach*. *Inter-network approach* is not considered because we only deal with the situation which jamming attacks occur in a network. Even though jamming attacks occur in multiple networks, it can be thought as the simple extension of the jamming-in-a-network case.

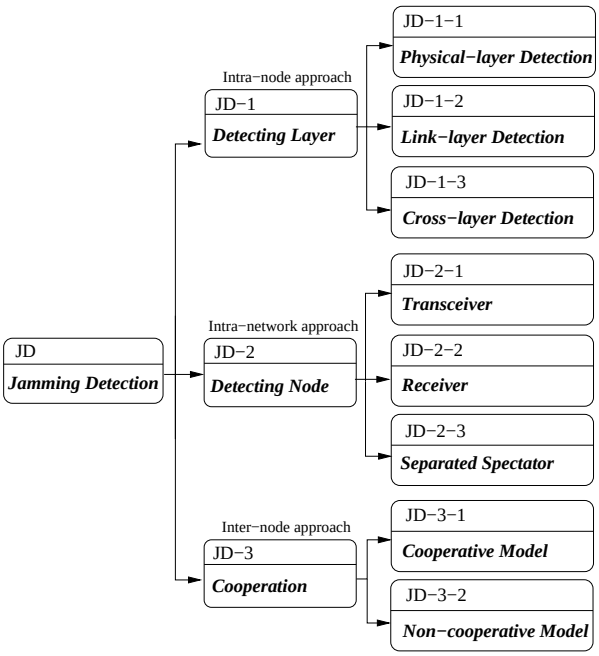

Fig. 4. Category of Jamming Detection

[JD-1] Detecting Layer

The detecting point of jamming in a node can be placed in each layer. The jamming in this paper is aiming physical and link layer, thus the detecting layer will be same. The detection on the higher layer than link layer is not accurate because it reflects the complex side effects generated by layers as well as the pure effect of jamming.

[JD-1-1] Physical-layer Detection

Most useful parameter in the physical layer which is able to be made use of is the signal strength. In [5], [9], [10], [27], the author suggests some methods which can distinguish the jamming signal from the normal signal. Basically, simple statistics like the average signal strength during a unit of time can be used. But, the author reveals that they can discriminate only the *constant jamming (JA-1-2-1)* from the normal traffic, not the *pulse jamming (JA-1-2-2)* or the *random jamming (JA-1-2-3)*.

Moreover, the detecting methods in the physical layer in principle are effective only on the *physical-layer jamming (JA-2-1-1)*. Most of *link-layer jamming (JA-2-1-2)* does not show any special signal pattern. Even if some *link-layer jamming* can try to send the bursty frames to the victim's node, the signal pattern of them is indistinguishable from the normal heavy traffic.

Another factor which should be considered in the physical-layer detection is the cost of implementation. Most of physical layer in wireless networks are operated by hardware. It implies that the cost to implement the detection algorithm of jamming in the physical layer is expensive. Contrastively, implementing an algorithm in the layer mainly operated by software, such as MAC, costs relatively low.

[JD-1-2] Link-layer Detection

The detection in the link layer originally intends to detect the *link-layer jamming (JA-2-1-2)*. However, the problem is that the link layer varies between wireless networks. For instance, the author in [5], [9], [10] presents the jamming-detecting method using the threshold of carrier sensing time, but it is only available to the link layer using CSMA/CA. In [22], the author introduces the detecting method of RTS/CTS jamming, which is available only in WLAN, by counting the number of RTS/CTS frames.

It is also possible to detect the *physical-layer jamming (JA-2-1-1)* in the link layer. The author of [5], [10] performs experiments to use PDR, which can be measured in most of link layers, for differentiating jamming traffic from normal traffic and reports that it is effective on the experiments. However, it is known that it still cannot distinguish between jamming and network anomalies like battery failure. The author again presents the detecting methods by PDR with consistency checks. When PDR is checked with signal strength consistency or location consistency, it successfully differentiates the jamming attacks from normal traffic or network anomalies. The jamming attacks used in the experiments are also categorized as *constant jamming (JA-1-2-1)*, *pulse jamming (JA-1-2-2)*, *random jamming (JA-1-2-3)*, and *reactive jamming (JA-3-1)* which has the sensing ability. In [27], the authors show that it is possible to detect *reactive jamming (JA-3-1)* by measuring PDR and Packet Detection Ratio (DR). The measured DR is still high under *reactive jamming (JA-3-1)* while PDR is low since the jamming results in the CRC-check failure in the receiver's link layer. For more generalized application of these approaches, further studies are required.

[JD-1-3] Cross-layer Detection

The mixed detection on the multiple layers is suggested in [28]. It first checks the carrier sensing time, the number of RTS/CTS frames, the number of NAV, and the number of collision. And then the channel utilization cost is calculated to discriminate jamming attacks from network anomalies. This is also based on IEEE 802.11 MAC protocol.

It is possible to develop the cross-layer detection in another type of wireless networks by adding specific link-layer detection to the compatible physical-layer detection if more studies make progress.

[JD-2] Detecting Node

The detecting point of jamming varies in the role of a given node in a network. A node in a network can play a role as a transceiver, a receiver, and a separate spectator.

[JD-2-1] Transceiver

Some characteristics of specific link layers enable the transceiver to be the point of detecting jamming. The carrier sensing time, which is mentioned previously, is measured in the transceiver which operates on CSMA/CA technology. This is because jamming attack influences on the transceiver by interrupting obtaining a chance to transmit. PDR value also can be measured in the transceiver by counting acknowledgement frames from the receiving node. Further studies are required to reveal whether other wireless networks which do not use CSMA/CA have the same effect that jamming attack gives directly or indirectly an influence on the transceiver.

[JD-2-2] Receiver

The detection in the receiver is the intuitively basic strategy because jamming attack originally aims at disrupting the receiver directly. Most of metrics introduced in *JD-1* can be measured in the receiver side. Relative to transceiver, the advantages from the detecting jamming of receiver are as follows: 1) It is more adaptable to general wireless networks even though the transceiver is not affected by jamming. 2) It responds to jamming attacks more quickly.

[JD-2-3] Separated Spectator

If the implementation and the execution to detect jamming in every transceiver or every receiver cost too expensive, we can consider the detection in the separate spectators. There will be the smaller number of separate spectators to monitor behavior of jamming relatively to the number of communicating nodes. Of course, some of communicating nodes in a network can act as spectators. This would be the applicable strategy in the situation, such as wireless sensor network, which the energy consumption is critical.

[JD-3] Cooperation

The cooperation between the detecting nodes is also one of the classification criteria. If jamming detectors cooperate with each other *(JD-3-1: Cooperative Model)*, detailed information about jamming, such as the exact range of jamming, the exact location of jammer, and the signal strength of jammer, can be obtained by exchanging their partial information. It is natural that the *cooperative model (JD-3-1)* is more useful than the *non-cooperative model (JD-3-2)*, but the cost in implementation and execution is high. Moreover, in order to cooperate between detectors, the separate communication channels which are not affected by jamming are additionally required.

APPENDIX C
MITIGATING THE JAMMING ATTACKS

Even though a jamming attack is detected, it does not mean it can be easily defeated. Without the aid of suitable mitigation mechanisms, there seems to be no way other than waiting until the attack is over. A jammer can be eliminated physically if the location of it is disclosed, but we do not include the physical mitigation of jamming in the category. It assumes that all the mitigation methods are performed by the communication nodes in wireless networks. All the mitigating methods of

jamming are examined in two different aspects, *behavioural intensiveness* and *adaptability to deploy* shown in Fig. 5.

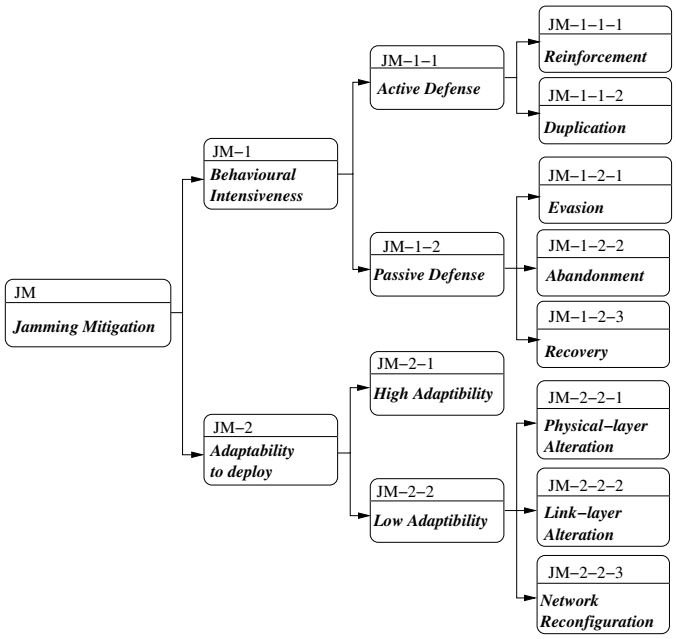

Fig. 5. Category of Jamming Mitigation

[JM-1] Behavioural Intensiveness

The mitigating algorithms of jamming can be grouped according to the level of their positiveness.

[JM-1-1] Active Defense

The active defense mechanisms are finally divided into *reinforcement (JM-1-1-1)* and *duplication (JM-1-1-2)*. Typically, the signal strength is the parameter to be used for *reinforcement*. As stated earlier, strong signal strength of transceiver can defeat the jamming signal. In [29], the authors adjust the transmission power sophisticatedly to defeat jamming under the non-isotropic jamming model. If the energy capacity is enough in the transceiver, this strategy will work to some extent. However, enhanced signal strength of transceiver causes unnecessary interference with neighboring nodes [10]. Moreover, most nodes in wireless networks have constrained energy practically. Further studies should solve these problems to make use of *reinforcement*.

Duplication means that using redundant information to resist jamming attacks. Forward error correction algorithms (FEC), such as Reed-solomon code, low-density-parity-check code, and turbo code, use the redundant bits to recover the partial damage of transmitted frames. This can also mitigate jamming attacks to some extent, but it still cannot recover the transmitted frames if too much corrupted bits are generated by severe jamming attacks, such as *barrage jamming (JA-1-1-1)* or *constant jamming (JA-1-2-1)*.

[JM-1-2] Passive Defense

There are three types of passive defense mechanisms: *evasion (JM-1-2-1)*, *abandonment (JM-1-2-2)*, and *Recovery (JM-1-2-3)*.

[JM-1-2-1] Evasion

The evasion techniques are trying to escape the geographical range of jamming or the frequency range of jamming. The former is called *spatial evasion* and the latter is called *spectral evasion*.

In [9], [10], the authors suggest the algorithm which the legitimate node can escape from the jamming region when the node is mobile. The authors in [14] assume the base-station is mobile in wireless sensor networks and presents the algorithm which can evade the jamming area efficiently in energy consumption.

The *spectral evasion* includes the traditional spreading techniques, such as FHSS and DSSS. There are some studies which develop the spreading techniques in terms of the jamming mitigation. *Hermes* prototype introduced in [30] combines FHSS and DSSS to defend against jamming attacks. In [31], [32], the authors suggest *Code Tree System* in spread spectrum to detect and evade jamming attacks by co-work between transceiver and receiver. And *Uncoordinated Frequency Hopping (UFH)* is proposed in [33] to exchange the shared key used for spreading techniques between two devices under jamming condition. The authors in [34] present approaches based on coding theory which reduce overall time required to verify the packets and reconstruct the original message in UFH. Apart from the spreading techniques, the authors in [9], [10], [35] present *Channel Surfing* which changes the communication channel when jamming attacks are detected. The duration of staying on a channel is relatively longer than spreading techniques. It changes the communication channel of all nodes or nodes in the jamming boundary with two different channels relay the jamming region and outside the region. In the latter case, the nodes should have ability to communicate through more than one channel simultaneously.

[JM-1-2-2] Abandonment

Even *abandonment* can be one of the defense mechanism. It does not mean that not doing anything against jamming attacks. In the respect of network, it gives up the jamming region and prohibits the traffic from flowing over the area by informing routing information to neighboring nodes. This prevents the jamming effect from propagating to the larger area. In [36], the authors map out the jamming region in wireless sensor networks and measure its performance by simulation. The fundamental problem of *abandonment* is that it is applicable only for the mesh networks, such as wireless ad hoc network or wireless sensor networks, not for centralized networks using base station or AP.

[JM-1-2-3] Recovery

This category differs from the recovery of lost frames by *forward error correction* in the aspect of a station. This means the network-aspect recovery from jamming damage. In wireless sensor networks, a lot of routing algorithms to re-route the damaged path have been proposed. The authors in [24] define *network dynamics* in mobile ad-hoc network, which is similar to *Newton dynamics*, and shows its application to recover from the damage by *mobile jammer (JA-3-2)*. The

authors in [14] present the strategy that combines the evasion and the replication. The replication is the switch-over of jammed base-station and it belongs to this category. Similar to *abandonment*, the recovery methods are suitable to mesh networks in general.

[JM-2] Adaptability to Deploy

Some of mitigating methods are practically difficult to be adopted since they require the alteration of standard protocols or the expensive devices or the reconfiguration of the whole network. On the other hand, some of them are relatively easy to deploy because they only uses the parameters which allow to be altered in the system. We name the former *low adaptable defense mechanisms (JM-2-2)* and the latter *high adaptable defense mechanisms (JM-2-1)*.

[JM-2-1] High Adaptability

The methods in this category should satisfy the conditions: it should not change the existing protocols or the legacy device or even the hardware configuration. These methods are highly adaptable to the deployed systems by only updating the given parameters (e.g. adjusting power, updating modulation and coding, routing information, etc.).

On the other hand, some studies such as [37], [38] build the theoretical model in the given system and draw the optimal strategy of jammer and network. Optimal strategy of network will be the mitigating methods of jamming attacks.

[JM-2-2] Low Adaptability

In contrast with highly adaptable defense mechanisms, all the methods leading too much cost of alteration are included in this category. The layers in a node may be altered more easily by the help of techniques such as software defined radio (SDR).

[JM-2-2-1] Physical-layer Alteration

In the examined examples previously, some strategies require the alteration of existing implementations. Both the case of adopting the spreading techniques into the device which does not have them and the case of having redundant channels to deliver information even under jamming attacks are included.

[JM-2-2-2] Link-layer Alteration

Most of methods to mitigate *link-layer jamming (JA-2-1-2)* are dependent upon the specific link layer and they require the alteration of link layer. In [4], [7], the authors present the link-layer jamming which is based on IEEE 802.11 MAC protocol and the solutions to mitigate it by alteration of link layer. In [23], [39], the authors introduce the link-layer jamming in the wireless sensor network and defense mechanisms against it. The authors in [27] introduce the original timing channel, which is sort of covert channel, under jamming attack. It requires that new layer called *4-Ounce Overlay* is inserted between the link layer and the network layer. The experiment is also performed in wireless sensor networks and it changes the link layer of wireless sensor nodes. In [40], the authors show the design of efficient anti-jamming schedules in wireless broadcast systems. Lastly, the authors in [13] introduce the link-layer jamming in WiMAX system and the solution using *shared authentication information*.

[JM-2-2-3] Network Reconfiguration

The mitigation methods of jamming in this category require the reconfiguration of whole network. The author in [41] suggests that the multiple base-stations make the WiMAX mesh networks more resistant to jamming than single base-station. In [42], the authors make use of the wormhole, which can exist in wireless sensor networks, to deliver the information from jammed region to neighbouring nodes. Multi-channel protocol [43] similar to wormhole also requires the network reconfiguration. The authors in [26] present the multi-dataflow topologies defense scheme to mitigate mobile jamming attacks.