Volume 7, Issue 4, April 2017 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

A Novel Approach to Detect Jamming Attack by means of Game Theory

Diksha Bhoyar
Project Scholar, Dept. of Computer Science and Engg.,
G. H. Raisoni College of Engineering, Nagpur (MS), India

Uma Yadav
Asst. Professor, Dept. of Computer Science and Engg.,
G. H. Raisoni College of Engineering, Nagpur (MS), India

Abstract---By considering a scenario where a complicated jammer continuously jams the network in a single channel WSN. Generally a jammer can control the possibility of jamming and message transfer range to cause maximum harm to the network termed as despoiled communication links. The jammer action halt when jammer node can be detected by monitoring node in the network, and warning message is transmit out of jamming region. Likewise the network also know the possibility of jammer .We focus the cases of perfect awareness by jammer and the network in order to study the strategy of one another . Also consider the cases where jammer network lack this information. We also consider different energy parameters of jammer and network. Two problem can be take into account as static jamming and dynamic jamming.

Keywords--- Jamming attack, Co-operative game theory, Data security, Key agreement.

I. INTRODUCTION

The elementary attribute of wireless sensor network that render them defenseless to attack is the major nature of shared medium. This broadcast the network to passive and active attack , these are different in nature and objectives. Generally the malicious node or entity does not take any action but attack node continuously observe communication which is ongoing state as eavesdropping so as to mediate with the preservation of privacy of the network that involved in the communication . Secondly an active attacker also involved in the transaction[5] . There are different terminology is used which depends on the attacker objective. The attacker can be called as misbehavior if the attacker abuse a procedure that have goal to get the performance benefits. The attacker is called as jamming , if the attacker or jammer does not operate the procedure parameter but has aim to disturb the network operation continuously and its depends on its reasons and consequences.[4]

Misbehavior be generated from tendency of wireless entity in order to improve their individual consequential usefulness to the decline by opposing from justifiable procedure operation at various layer. The usefulness is present in terms of extreme energy or feasible throughput on a communication link. In order to preserve the energy expenditure of its own transmission, the case arises if a node refuses to forward message from other node. The another case arrases when one node prevents other nodes from gaining the access of channel and from rerouting the message to the sink by egotistic management of the access control.[9]

The interaction model apprehends improbability of attacks and case of intelligent attacker that extend its detection. Jammer can wireless transmission and can happen accidently in the form of intrusion at the receiver side. Basically the jamming attack is very effective in number of cases (i) there is no special type of hardware is used to launch the attack (ii) the attack can be implemented by simply listen the open shared medium and probability in the frequency of the network. (iii) if attack is launched judiciously it can show the way to considerable benefits with small amount of incur cost for the attacker. The impacts of jamming attack typically aims at the physical layer and are accomplished by means of a higher transferring power signal that disturb a communication link. Predictable resistance techniques against physical layer, jamming attack depends on spread spectrum that can be exhausted energy consuming. Jamming attack also takes place at the access layer in this, an challenger either corrupt data packet or assets the channel for the maximum number of slots, therefore other nodes in the network have low throughput . The study contain the problem of a justifiable node and a jammer that transforming into common receiver in a game theoretic analysis. The different type jamming attack manipulate network layer by corrupt packet inoculation along a transport layer.[3] Generally attacks in the network can be detected by observing the IP port and by using various detection technique. The work uses game theory in order to detect attack and computational cost.

Wireless sensor network are susceptible to malevolent attack. There are several reasons account for this malicious attack. Firstly sensor network are established in the distant region and unattended. Malevolent nodes may usually be inserted into the wireless sensor network and accomplish different attack such as dropping of packets, injection of unwanted data.[2] The wireless medium is open and it is shared in the radio transformation and therefore referred to as radio interference. There are number of counter step based on cryptography can be used for amplify the security of wireless sensor network. These counter steps are effective for attack there is a transmission of high-power radio signal. For a wireless sensor network with a single channel the sensor node within the interference range can be suffer from degradation of performance of data if the jamming signal are transferred on the radio interference channel.

1.1 Jamming Counter step

For the communication of jamming attack there are three ways are available : jamming passive resistance , jamming revelation, jamming extenuation. The equable and adequate way in order to avoid the jammer is to moving out of the jamming region and by interchange the communication link and the packet cannot be affected by the jammer. Instead of the jammer adequateness, the most of jammer is never possible in most of the wireless application . The effluence of the jamming detection mainly depends on the causes of the network parameters that is quick deactivation of the jammer that can be taken. This place the limitation in the application of jamming detection where there is no middle action is necessary.[11] The main common measure to the jamming is to extenuate the impact of jammer by using anti-jamming communication technique contain highly directed antenna spread-frequency spectrum, and error-correcting codes. Periodicity hopping spectrum and direct successions widen spectrum are the common anti-jamming communiqué techniques that enable the sender of the message to increase signal in time such that it is transmitted in the unpredictable to the jammer. Basically attacker cannot physically segregate a device, attacker alter or delete the message and it is restricted by the interference with the message transformation and hence the performance can be reduces. The gaining of the performance present the cost of the attacker in order to jam the transmission line in terms of energy consumption and it is in the order of 100 to 100 times the second cost. Therefore the chances of the successful interference of malicious jamming attack are because of attack is not much powerful if attacker wants to stay undetected.

1.2 Contribution

There are main four contributions:

We deal with difficulty of anti-jamming communication techniques with shared private key signature and establish the interaction model and key signature can be generated.

We suggest a game theory analysis as a solution to deal with the problem of high frequency based communication technique that easily supported by the length of message which is rely on key signature. We develop the interaction model contain some node as a jammer node and perform continuous jamming which allow the permutation of block channel and probability of jammed packet is the utility of length of packet and packet training.

II. JAMMING ATTACK

In this attack, the malevolent node advertises fake direction-finding information such as it has the straight and steady path to reach the intention, and cause the other high-quality nodes to create the path throughout this malicious node. Once the path is recognized, then it either drop the data packets, or change the direction-finding update packets. Jamming attack is of two types: [6]

Solo Jamming Attack: A Jamming attack basically means a malicious node declare itself as having the straight path, but it does not ahead the packets after begin the path. A single jamming attack be able to easily occur in the network. This is shown in the figure 1 given below.

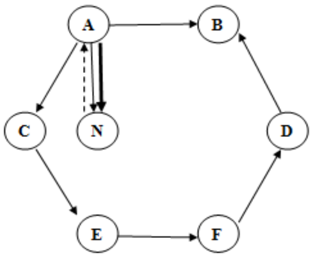


Figure 1: Single Jamming Attack

Co-operative Jamming Attack: In attendance can be other than one node which is co-operating with the solitary node attack creation them undetectable from the new truthful nodes. The cooperative attack is shown in figure 2 given below.

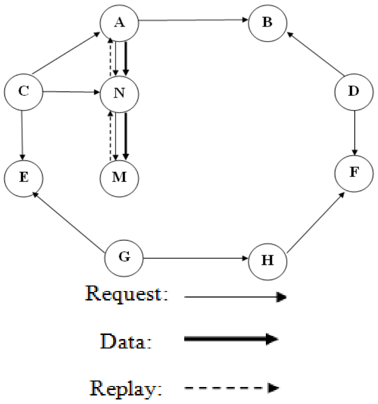


Figure 2: Co-operative Jamming Attack

III. ANTI-JAMMING COMMUNICATION WITHOUT DISTRIBUTE SECRETS

The unblock environment of wireless communication make them predominantly susceptible to message jamming attack. The major goal of this attack is to intercept devices from alternating any useable message or data by producing interference with in the communication. Possible communication, basically jamming attack consist of total signal destruction, variation and jamming also there is the insertion of fictitious signal.[5] Spread spectrum techniques are the counteragent against jamming attack communication. In all spread spectrum techniques contain secret key which are shared between the communication link. The secret key permits the sender to distribute the signal in time therefore the signal in time therefore the transmissions is unpredicted for a malicious party therefore it reduces the channel of interference. Basically required secret key must be shared between the communication link generally it is unpredictable transmission stuck between sender to the number of unknown receivers. Out-of-band is the code distribution technique can be used for the fulfillment of shared secret code. The out-of-band technique can be suffer from scalability problem.

At the time of deployment of communication all the devices are not known because it is not superior to keep trust on devices. The devices do an agreement on a secret key using wireless channel. For the execution of key establishment protocol require the shared secret key. There is a dependency between key establishment protocol and jamming refused communication. Also there is dependency between secret key and spread spectrum. This is called as anti-jamming or dependency of key establishment. Basically trusted authority issue some security key certificates which is hold by the devices, but they need to perform communication to establish a secret key. Figure 3 shows the dependency cycle of key establishment protocol used in the key agreement.

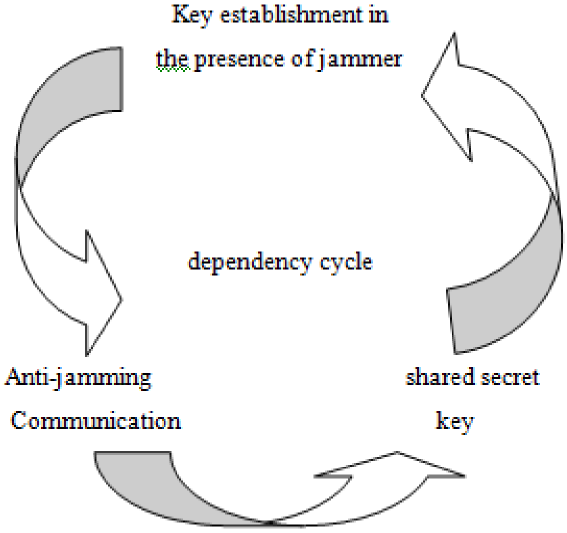


Figure 3: key establishment dependency cycle protocol

If two nodes in the network not share key and they want to execute key establishment protocol in the presences of the jammer, then there is a use of jamming refused communication technique. Dependency chain of key establishment protocol can be show in figure 4. In the scenario of dependency chain the secrete key can be shared in the presence of jammer in the network and anti jamming communication can be built in the time sequence. Secrete key can be shared on the basis of timing sequence because the jammer can jam the network but timing sequence cannot be jammed.

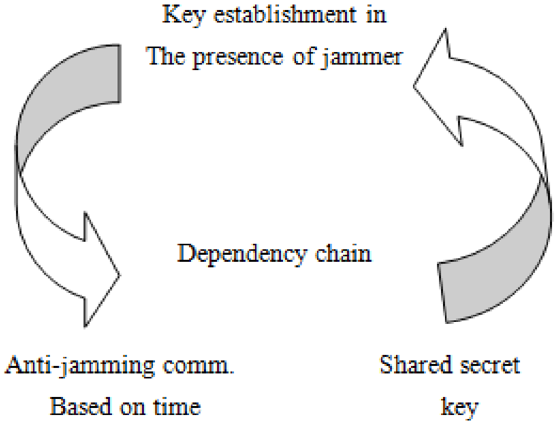


Figure 4: key establishment dependency chain protocol

Time factor can be used that permit two nodes to execute key establishment protocol in the presence of jammer instead of two parties not share the secret key.

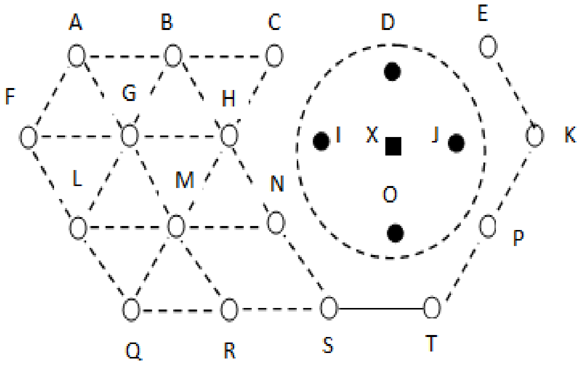
IV. ESTABLISHMENT MODEL OF JAMMING ATTACK

In this section there is a basic outline of wireless network and jamming interaction model

A. Network model

There are various number of wireless networks have appear, the are from wireless sensor network , mobile network to mesh network. The extensive range of preference imply that there are too many different directions are available that tackle the problem of jammers.[10] Construction of standard approach that works diagonally all modification of wireless network is unworkable. Therefore as a preparatory point we focus to mold our solutions to a grouping of wireless network with some properties. Figure 5 can explain the whole network implantation.

Motionless:- Assume that the deployment of wireless network and location of each devices are unchanged. Consider the scenario of wireless devices for project work.



■ Jammer ● Jammed nodes ○ Boundary nodes

Figure 5: Jamming scenario with jammer, boundary nodes and jammed nodes

1. *Near-by resident-aware* :- There are number of near-by resident are present for each node in the network and each node maintain its own near-by resident that records the information of neighbors, information activeness of node and respective location. These neighbor tables are maintained by routing protocols.
2. *Locality-aware:* - In the network each nodes known its own location co-ordinates and its near-by resident location. This is common consideration because many number of application require localization services.
3. *Detection of jammer*:-Focus on the location of the jammer if the jammer is detected. There are number of jamming detection technology are available and they are ranging from simple parameter testing to complex stability. In this paper, we use game theory model for the detection of jammer node.

B. Jamming model

In order to jam wireless communication many different strategies are there that perform jamming. In constant jamming attack, jammer continuously emits high energy signal and jams the wireless channel. In reactive jamming attack wait for the channel to become idle, and start higher energy signal as soon as channel is idle and message can be destroyed at the receiver.[11] Even though the miscellany of different attack, the penalty of jammers are same. The nodes which are near-by jammer, the communication between them are disrupted and cannot communicate with other near-by neighbors. But the nodes which are distant from jammer are not affected by jamming attack. The jammed network interaction model can be divided into three regions : jammer, boundary nodes and jammed nodes. A jammer can be situated in a jammed region it cannot collect any packet from any its near-by resident. Boundary nodes are at the border of jammed region. The categories of nodes in the network are the liability of jammer detection techniques. In this paper we construct models for static jammer and dynamic jammer.

V. GAME THEORY MODELLING

The main objective of this paper is to perform game theory model for the detection of jamming attack. Game theory can be use to analyze the different behaviors of jammer that jam the channel. The paper also presents many detection mechanism of jamming attack by using game theory. Jamming attack can be model as a playing game between two players called as jammer and nodes in the network and they have different objective. Basically jammers are the player who prohibit and refuse the access of wireless channel for users in order to jam communication link. Nodes in the network work as a communicators called as communicator players have objective to adequately use wireless channel in order to increase throughput. Here there is a modeling between jammer and nodes in the network called as monitoring nodes.[13] Monitor node are the main player that is responsible for the detection of jamming attack. The interaction model between jamming attack and its detection can be modeled as a two players, non cooperative game. In set of players one can be considered as a jammer and other as a monitor node. For a particular time interval different model can choose to continuously informant to the wireless channel. For the detection of jamming continuous monitoring can be used but their result in higher energy expenditure. For occasional monitoring there is less energy expenditure.

VI. IMPLEMENTATION PLAN

To increase the source node privacy and security, game theory approach can be used in order to detect an jamming attack. Message can be transferred from source to destination likewise jamming attack can be detect. Basically two approach can be develop as static approach and dynamic approach. At the source side message can be transferred by using local IP address of source system and the respective message then transferred in the network deployment region.[14] In network interaction model some node can act as a jammer, some of those are boundary nodes and others are monitoring nodes.

In static approach, each packet is transferred to the destination from the source side. Packet can contain authenticate data of any size of packet that can be transferred to the destination node and likewise signature key can be generated. Signature is a private key that can be randomly depends on the size of packets and number of nodes contain on the route of transferring packet. At the destination side signature key can be verified and message or data can be successfully delivered.

In dynamic approach any data or message can be goes through source, router and reaches to the destination. At the source side message cab be recorded by using IP address of source system and message or data can be transferred by connecting source to the connecting server. Then message or data can be entered in the network there are different nodes are present in the network but starting node or monitoring node can decide that which path can choose to transferred message through network. Here game model can be developing. In these some nodes are attacked by jammer, firstly message come at the start node then start node play strategies to transfer packets. The game strategies can be played by each node in the network. The strategies play by sending probe packet first, there is no data content in the probe packet. Each probe packet is transferred to the sink node from the monitoring source node until probe packet reaches to the receiver side.

Secondly forwards that probe packet by pre-establishing the path from destination to the source. Each the sensor node can select one of the neighbor's node that is not recently visited. Then actual message can be transferred, if there is any jammer in the network then node failure can occur. Then the network can choose another path for sending the data to the destination. At the destination side signature key can be verified and message or data can be successfully delivered. Signature key can be generated that can be verified at the destination side and data can be collected or receive at the destination successfully.

VII. RESULT

Implementation result can be shown by graph in which different metrics take into consideration. Signal strength can be calculated between static and dynamic approach in which static approach have less signal strength in compared to dynamic approach. The game theory model can be used to identify the safe communication path over the network . The game theoretic model can perform the interaction between jammer node and communication node. This is the situation in which two wireless node interfere the transmission line as soon as it detect the packet transfer activity. Jammer disturbs the data enclosed in the container which is jammed but its particular timing in sequence cannot be blocked. Therefore by using information of timing channel the data or the packet can be delivered to its destination. Figure 6 shows ratio of signal strength between average signal value and number of nodes in the network. Static and dynamic approach can be build to detect reactive jammer in the network. The model based on the game theory approach that contains static approach and dynamic approach. The model can improve the network interaction by sending packets successfully in order to improve the network life. The proposed model can verified under different parameters contain speed, signal strength, network capacity, packet delivery ratio, and signal to interference ratio. In addition, we have presented the concept of evolutionary game using a group policy/authentication to resist the intelligent attacks which do not use pure strategies. We expect astounding results after applying this model, such as reducing the number of dropped packets, promoting the efficiency, increasing the security level, managing the interactions between nodes, rapid attack detection, regenerating (based on the evolutionary nature of the game) and intelligent strategies against new manipulations of attacks, with the aim of producing powerful trust model based on game theory.

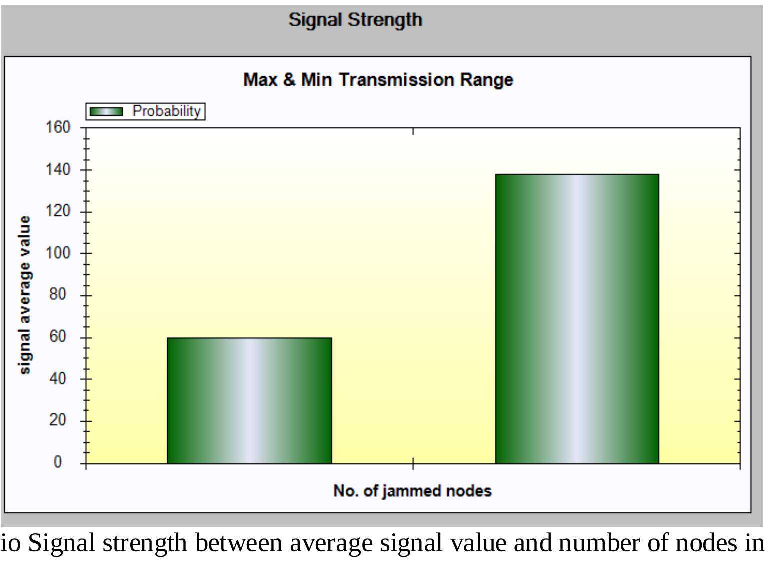


Figure 6: Ratio Signal strength between average signal value and number of nodes in the network.

Packet delivery ratio calculated by maintaining routing table in static routing and in dynamic routing PDR is the demand routing . PDR is the ratio of packets that are successfully delivered in the destination with respect to the packets that are sent from source side. PDR ratio of static and dynamic approach shown in figure 7.

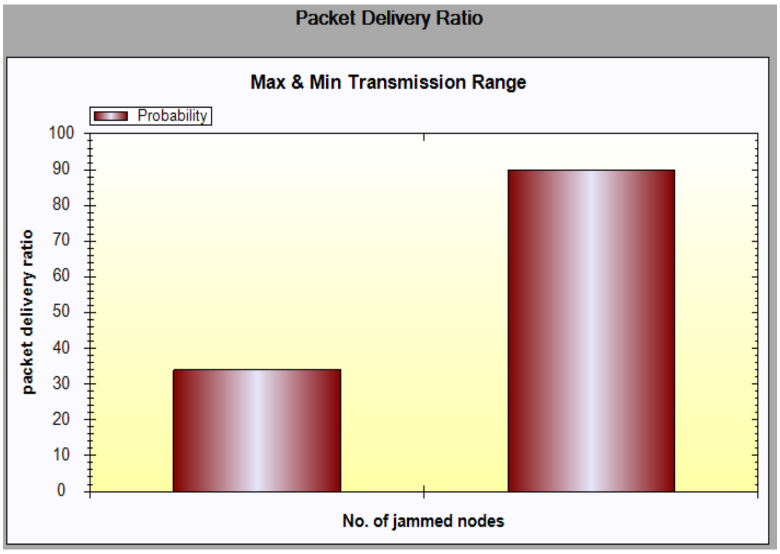


Figure 7: Packet delivery ratio

VIII. CONCLUSION

Therefore in this paper, data security can be provide by means of game theory. We implement interaction model between jammer and the sensor node in the network in order to detect jamming attack. Its challenging task to modify game theory and to identify the jammer strategy in the network. Static and dynamic approach can be build to detect reactive jammer in the network. Therefore in implementation of jamming attack using game theory, data security can be providing by means of game theory. We implement interaction model between jammer and the sensor node in the network in order to detect jamming attack. It's challenging task to modify game theory and to identify the jammer strategy in the network.

REFERENCES

[1] Ling Shi, Peng Cheng, Jiming Chen and Daniel E. Quevedo, "Jamming attack remote on state estimation in cyber physical system: A game theoretic approach." IEEE Trans. Wireless Communication, Vol.60, Issue 10, Page No.0018-9286, 2015

[2] L. Galluccio, G. Morabito, and S. Palazzo, "TC-Aloha: A novel access scheme for wireless networks with transmit-only nodes," IEEE Trans. Wireless Communication, Vol. 12, No. 8, Aug.2013.

[3] S. D'Oro, L. Galluccio, G. Morabito, and S. Palazzo, "Efficiency analysis of jamming-based countermeasures against malicious timing channel in tactical communications," in Proc. IEEE Trans. Wireless communication , Vol.14,Issue-5, Page No.1566-1276,2013.

[4] D. Yang, G. Xue, J. Zhang, A. Richa, and X. Fang, "Coping witha smart jammer in wireless networks: A Stackelberg game approach," IEEE Trans. Wireless Communication, vol. 12, no. 8, Page No. 1536-1276, Aug. 2013.

[5] G. Morabito, "Exploiting the timing channel to increase energy efficiency in wireless networks," IEEE J. Sel. Areas Communication, vol. 29, no. 8, Sep. 2011.

[6] S. Anand, S. Sengupta, K. Hong, and R. Chandramouli, "Power control game in multi-terminal covert timing channels," IEEE J. Sel. Areas Commun., vol. 30, no. 1, pp. 44–53, Jan. 2012.

[7] S. Periyanayagi and V. Sumathy, "A Swarm SBased Defense Technique for Jamming Attacks in Wireless Sensor Networks," International Journal of Computer Theory and Engineering, Vol. 3, No. 6, December 2011.

[8] Neha Thakur and Aruna Sankaralingam, "Introduction to Jamming Attacks and Prevention Techniques using Honeypots in Wireless Networks," International Journal of Computer Science and Information Technology & Security , Vol. 3, No.2, April 2013.

[9] S. Raja Ratna, R. Ravi, "Survey on Jamming Wireless Networks: Attacks and Prevention Strategies," International Journal of Computer, Electrical, Automation, Control and Information Engineering Vol: 9, No:2, 2015.

[10] Ritu, Pooja Ahlawat, "Game Theoretic Modeling of WSN Jamming Attack and Detection Mechanism," International Journal of Computer Science and Mobile Computing, Vol. 4, Issue 6 June 2015, Pg 648-653.

[11] Vinoba, Chithra, "The Study of Game Theory in Wireless Sensor Network," International Journal of Emerging Trends and Technology in Computer Science, Vol. 3, Issue 5, September_October 2014.

[12] Padmal Saidesh kumar, "Designing of Game Model for Achieving of Flexibility Towards Jamming Attack, " International journal of innovative technology and research Vol.4, Issue No. 3 April-May2016

[13] 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

[14] R. Saranyadevi, M. Shobana, and D. Prabakar,"A survey on preventing jamming attacks in wireless communication," Int. J. Comput. Appl., vol. 57, no. 23, pp. 1–3, Nov. 2012.

[15] W. Xu, K. Ma, W. Trappe, and Y. Zhang,"Jamming sensor networks: Attack and defense strategies," IEEE Netw., vol. 20, no.3, pp. 41–47, May/Jun. 2006.