ISSN:2348-2079

Volume 4 Issue 6

International Journal of Intellectual Advancements and Research in Engineering Computations

FRAGMENTS SIGNATURE AND TRUST REGISTER TECHNIQUE FOR DETECTION OF JAMMERS IN WIRELESS SENSOR NETWORKS

[1]S.Sathishkumar, Research Scholar, Annamalai University, Chidambaram, Tamilnadu, India.

[2]A.Senthilkumaar, Professor, Annamalai University, Chidambaram, Tamilnadu, India.

Abstract

Wireless networks, the dominant and successful networks of today, defined a flexible approach of providing service to the nodes anywhere and anytime. Either autonomous or client machines are distributed spacially to perform its prescribed functions by the base station. The data collected from the environment, considered to be of sensitive importance, have to be ensured to reach the right end. When deciding a framework of the wireless networks, a number of conerns have to be concentrated. Traffic of the data packets, congestion control, and prevention from attacks of any kind, detection and tracing back of attackers will be the prioritized actions. Denial of Service attacks, an attempt to degrade the network's resources such as bandwidth and memory, target a single machineto prevent it from getting or sending the data to the base station. The paper introduces a novel approach to monitor, communicate and determine if there is any attack within the networks. The proposed protocol will be ensuring the confidentiality by enabling a three times check for the originality of data packets. When the system doubts a data packet, signatures are checked in three registers, one from the sender, intermediate and the destined node. Any packet without these signatures will be regarded as an attack packet. The advantage of this method is to counter a low profile DoS attacks, which has evolved into a new type of attack for minimal evidence of an attack.

Keywords: Jamming, Detection, Signature, TRUST Register

Introduction

A wireless Sensor network comprises of a number of nodes established in a region which limits the active participation of human beings for examination [1]. Sensors range from size to the metrics it senses. A network will comprise of numerous sensors for sensing and delivering data to the base station. Wireless Sensor Networks succeeded much theoretical impossibility and simplified the architecture of the networks implementation. The networks established using traditional approaches has significant conditions on extension of the nodes or sensors and connecting the nodes via physical cables. The expenditure and constraints were too difficult to be obeyed in the traditional approaches of implementing a network. On the other hand, the wired networks were too stringent over the attackers too. The entry procedure of any user is clearly monitored which restricted many imperfect attackers. Speaking of the attackers in the wireless networks in internet services specifically, there has been no limit to be defined. High accessibility and usability made the wireless networks a bit insecure to that of wired networks. Limited access with physical links is thus a secure method to protect the resources of a network from external users. But in a view of a large organization, there is a serious necessity of providing access to multiple users with easier protocols.

The framework of the wireless networks is to provide the services to the user irrespective of the location or the need of a physical medium. The urge of this flexibility is opted by the users on the run, to access the resources of the concern with provided authenticated identities. The need of fixation of a node in a stated place, communication links via physical cables and limitations to the capacity of the medium used, promoted the concept of deploying wireless networks. The wireless technology eliminates the difficulties of a wired network by allowing the user to access the resources with no limitations. Wireless sensor networks have a number of thousand nodes or more distributed in remote locations and all nodes are capable of requesting service simultaneously.

The important factor is that not all the users are legitimate requestor of a service. There are outsiders who perform activities which disturb the security and integrity of a network [1]. Their goal is to bother the functionality of an intended user and the services provided by the network either by blocking, distracting or by flooding the medium [5]. The attacker acts in between two users to prevent them from communicating. The attackers learnt the ways to hide from the detection algorithms by acting as a legitimate user (spoofing) or making the network administrator to believe that there is no attack in the network.

There may be attackers internal to a network, that is, a legitimate user could also attack the network functions for his particular reasons [3]. The wireless networks are prone to a much higher rate of attacks than the wired networks. Any attacker who gains access to a network for altering the default activities is a serious threat to the data of high confidentiality. The detection algorithms have not matched to the speed of detecting the attack in earlier stages.

This report studies the jamming attacks of the attacker by various means and analyses the effects. The motivated study is to make sure that the jammers could be used for constructive mechanisms of conserving the security of a highly important network which cannot be compromised at any cost.

The jamming attacks were introduced in the military applications for transmitting the commands securely by blocking the means of eavesdropping. Then the attacks started to roam in the day to day life in radio signals, in gaming theories and to the extent in social networking. Recently a social network was blocked from its service to thousands of users. The origin of the jammers was a very simple strategy to perform the intended function. The initial jammers are categorized into four types based on their transmission of the disturbing signal [2][4].

The **constant** jammer transmits the jamming signal of high transmission power to the medium of communication regularly till the jammer is dried out of power. The constant jammer continually sends a meaningless signal just to block the network. In case of CSMA networks, prior to the transmission all the nodes would check whether the medium is free or not. The medium would never be found idle to allow the legitimate transmission. Hence the jamming attack succeeds. But considering the energy factor of the jammer, without any external power supply, it works till the battery is dried off. Once the charge is used completely, the jammer dies and the original service begins.

The **deceptive** jammer resembles the constant jammer in its activities and differs from the signal which it sends to block the intended service [7]. This type of jammer uses the actual resource messages to be transmitted for the attack. The network users never get a chance to detect the whether the service is an attack or from the original source. The receiver would allow the transmission and the original data packets from the right source are blocked since the channel is in use. This type of jammer was introduced to evade from detection mechanisms. But the energy of the jammer is the drawback, resulting in limited time usage.

The next evolution of the jammer is the **random** jammer, which was proposed with the idea of conserving the power whenever possible. The jammer is programmed to be active for a defined time and goes to sleep for a defined time. The jammer transmits a random signal such as a noise signal or any other signal for sensing the medium to be busy for a unit of time and remains idle for a period of time alternatively. This facilitates the longer lifetime of the jammer.

Eliminating the limitations of all other jammers, the **reactive** jammeris an intelligent mechanism. The jammer is activated to transmit blocking signals only when the original messages are to be exchanged. Otherwise the jammer goes to the energy conservation mode (switched off). This method is far better in conserving the power of the jammer. These types of jammer merely send a message for colliding with the original message. On collision the legitimate message is dropped.

These jammers discussed are the devices that act external to a network, on the command of attacker related or not. There are also cases in which the internal users of a particular network selfishly act to block the services of the other users. They selectively jam the networks by altering the messages of high importance such as TCP or messages of routers. These attacks are said to be **selective** jamming attacks. Instead of blocking the communication channel, the messages and their contents are altered.

Motive of Jamming

The ultimate aim of jamming is to congest the communication channel with unwanted signals, never leaving a chance for the legitimate users to access the same [1][3][5]. The channel is blocked till the waiting queue is filled and the fore coming messages are dropped. Otherwise jamming retards the complete reception of packets at the destination. The whole message could not be retrieved unless all the packets are received.

The detection algorithms work hard to identify the attack and try to prevent the possibilities. However the new attacks are capable of overcoming and eluding the algorithms to continue their mishap activities. The additional motive of a jammer is to hide from the

detection algorithms and proceed with the blockage of signal [8][9].

Power management of the jammer is apart from the normal operation, but still needs certain consideration. The efficient way of using the jammer enhances the period of attack to the network. The jammers are said to have enough power as much as less than 1000 times than the legitimate transmitter to block the service. Yet energy efficient jammers are preferred and employed.

Every jamming attack selects a specific area for attacking and those techniques are discussed as follows. The jamming attacks are prominent in blocking the channel by means of an undesired signal. The CSMA networks checks for the channel to be idle and waits till the link is freed. The user finally gives up and thus the service is blocked. This jamming attack concentrates on the bandwidth and frequency of the channel. Jammers of this type are the first to be of the attack. The aim is to forward a signal equivalent or more powerful than the legitimate signal. This type originated in the broadcast of radio signals. But these attacks are easy to overcome if the frequencies are changed by the sender. Hence the need of more serious attacks rose.

The current jammers are made to block the messages that are supposed to be in place. The RTS/CTS messages constitute a pair in which either cannot be lost for a complete communication. The jammers wait for a RTS message to be transmitted and then block the other. The network waits for the reply and retransmits the message again. Till the message is blocked by the jammer, repeated transmissions occur until user identifies the reason. Similar to the blockage of RTS/CTS messages, the data packets are prevented from reaching the destination [16].

Jammers are also well versed with altering the authentication and claiming to be the part of the network by spoofing. Proposing reasonably allows the attacker to gain access to the services of the network. The authentication messages from new users are distracted from reaching the module for authorization. The module then disapproves any incoming request messages and thus new users are rejected.

Apart from the external attackers, the selfish users internal to the network could also jam the services and functions of the network. Being an authorized user of the network, attacker will use the medium for a considerably long time, making all other users wait for their turn to transfer the messages. These discussions have stated the models of jamming attacks in the field today. There have been detection and prevention theories proposed to control and mitigate the jamming attacks. Countermeasures are based on the encryption of messages and securing the channel by high power transreceivers. Yet the jamming attacks are significant enough to succeed the mechanisms [13].

Countermeasures include the verification of the channel traffic at regular intervals, comparing with a threshold value of normal traffic and traceback methods to identify the attacker. But there are still no successive methodologies to completely eradicate the jamming attack. These countermeasures cannot be the solution to all the available attacks and newly developed immune attacks.

The following section discusses the constructive ways of using jammers in a network. The same functionalities of a jammer could be proved to be fruitful in terms of positive approach. Applications of highly important message transfer cannot compromise on the attacks. Jammers could be used for preventive measures in military and health care applications where a simple attack leads to catastrophic effects over the entire nation.

Evolved Jammers

Jamming is achieved by flooding the bandwidth or exhausting a network with numerous requests such that it loses concentration on the priority and the order of execution. The service provider will get confused on which to respond first or gets crashed in most cases. Requests of different varieties would not provide a chance for the network to react and thus crashes the whole system [13][15].

One has to clearly understand the difference between the congestion in a network and Denial of Service (DoS) attacks. Legitimate requests from multiple users cause congestion. Congestion can be removed by making the requests wait till the state changes. If the intention of the requests sent to the server is defined for making them wait indefinitely, then it is called as the DoS attack. The requests remain unanswered till the congested state is removed, yet the jammer would continuously jam the network by sending in false requests [15].

The internal jammer or attacker is capable of observing the activities at every moment and act accordingly. They need not be active for a long time to attack. Aware of the detection and prevention strategies, the attacker will stay low till the network functions are degraded. The internal attacker would pose a threat in any of the following means.

Sybil attacks are used to gain the control of the networks by compromising a number of nodes with multiple identities. The internal attacker avails the information of the entities and their session details. With the information on the login ids and password the same internal attacker may act as multiple entities and possess as many sessions as possible. Finally the attacker would be able to misuse the resources of the network. The network monitor would validate on the identities of those

multiple nodes but not doubt their source. Resulting in a blockage of services to the original users who would be rejected to login and obtain their service.

The next type of attack is the node replication attack by an internal jammer, in which the nodes are created repeatedly with the intention to disturb the original routes in the network. The nodes are replicated with the same identity such that there are numerous nodes with one identity. When the route is established, there is no surety that the original node will be assigned. The replicated nodes would lead to a false destination thus jamming the original route. This attack is severe if the messages to be communicated are of high importance. The internal jammer would be aware of all the identities of every node on the network.

Wormhole attacks are the next kind of attacks of an internal jammer. The packets transmitted at the source node are recorded by the attacker. The jammer would then create a dedicated pathway for the copy of the packets to an attacker's destination node. This method would disturb the confidentiality of the message packets. The worm holes can be also created in between the original source and a duplicate destination by assuring it as a true destination node. Jammer need not know the keys for breaking the encrypted message for posing a threat since the packets are jammed from reaching the destination which is already an attack. Being an internal attacker the keys used for encryption and decryption would be open to all members of the network. The route request and response messages are the primary concerns of the attacker. Without a secure channel for communication the messages cannot be ensured with confidentiality. Immediate analysis and detection of these wormholes is absolutely necessary to prevent huge data loss.

These fore mentioned attacks concentrate on compromising the nodes and their activities. The next type of attack greatly concentrates on the messages of high importance. A Selective jamming attack wait for the transmission of high significance messages and then block them from reaching the destined nodes. Blockage of these messages requires much less effort than the former type of internal attacks. The internal jammer is well informed about the time and types of the important messages unlike the external attackers.

Taking into consideration of the applications and efficiency measure of the sensors, they can be employed in a constructive way.

The interference of signals, exclusion of noise and distorted signals needs to be removed for obtaining a good quality and security over the legitimate signals. Prevention of attacks through implementation of jammers is possible and without detection enables the source and destination to promise a reliable channel for communicating. The jammers have evolved into low power, energy efficient and are capable of high coverage regions. Jammers introduced in the military applications had the motive to prevent the adversary from eavesdropping and altering the high command to mislead the aircrafts, launch of missiles etc.

Jammers in use today are far developed than the traditional usages. Mobile applications such as cellular phones, Wireless LAN services have been disturbing one or the other. In schools and other educational institutions mobile signal jammers are employed for offering a dedicated environment for the original purpose. The holy places are too under attack by these users. The sacred activities are often disturbed by the human friendly services which enforces the implementation of the positive jammers. The selfish behaviours of some users are intolerable for the important services in civilian applications. To mitigate the jamming attacks of all kind, positive jammers are in sensible urge to be implemented.

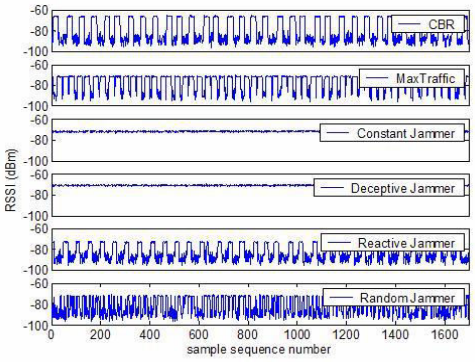


Figure 1: Activity of Jammers

The Figure 1 shows the activity of various jammers explained already.

The case of distributed jammers grouped into a network acts against all the odds. Distributed jammers are the latest development of jammers, in a size invisible to the naked eye, forming a larger boundary of coverage area and energy efficient. Understanding the importance of the war field, the communication has to be secured by all feasible means. The distributed jammer networks resemble a formation of dust, but performing the function to disrupt and suspend the attacker's signal from every nook and corner. The dust of jammers also possesses a low self interference rate in order to avoid collision of the same motive jammers.

Although the civilian applications are simple in words the disturbances are unbearable. Considering the healthcare applications, emergency situations needs the best quality for proper analysis and recommendations of the patient in last minutes. Mostly the jammers are unaware of the location of attack which he initiates. Hence the jamming attacks need serious countermeasures at once [9][10][11][12]. Denial of Service has to be

provided to the attacker himself to conserve the integrity of the network applications.

NETWORK MODEL

A group of N number of sensors within the same transmission range serving under the same Base station [16].Clustering is done to significantly reduce transmission cost and each cluster will be assigned with a dedicated centre Head. The Centre Head will be appointed on the criteria of with maximum battery capacity and in uniform distance from all other nodes. Omnidirectional antennas will be the communication medium with k range of frequencies. The clustering will offer a standard distribution of energy to and from the base station, other nodes, and between cluster Heads eliminating the exhaustion of some nodes when needed the most. Every sensor is programmed to report to the cluster head in regular intervals regarding the status of the respective time. An assumed content of a sensory node is shown in the Table 1. The sensor ID defines its identity, the timestamp defining the initiation of messages from the network model and the status holding the flags mentioning the mode of operating. The message will be the space for any optional statements from sensors informing the base station or cluster head about the remaining battery power.

Sensor ID	Timestamp	Status	Message (Optional)

Table 1: Sensor Data

ATTACKER MODEL

The attacker as mentioned before could be a node waiting for the service or request to be transmitted and responded [15]. On the medium, when a packet is caught by the attacker node, it may try to read the contents or alter them.

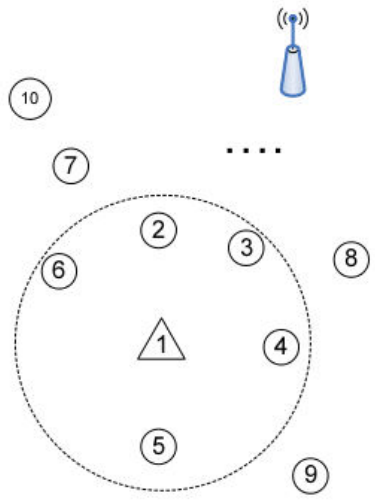


Figure 1: Network Model: Cluster Head with associated nodes

A sample network model is shown in the Figure 1. Considering the impact of confidentiality and importance of the same in military or any other defence organisations, prevention of such activities should be eliminated [21]. The proposed solution will generate a key based on the identity of the node initiating the message and will be delivered with a timestamp of the intermediate messages. The strength of jammer is unknown and predicted to be higher than the other nodes serving in the network [19].

PROPOSED SOLUTION

A message initiated from the source node carries a highly confidential message, upon deciding on the destination, a path is selected and start the transmission. The IP address of the initiating node will be registered into a table called TRUST table in the cluster head. IP and the time stamp is entered into a NXN matrix. A simple or confidential SCAN pattern will be applied on the matrix to generate a key Pattern. It will be communicated to the destination for decryption process.

scan(pos1-pos2, pos2=next)
next=(path (S-D))
pos1>0,pos2>pos1, next!=pos1,pos2 (iterative)

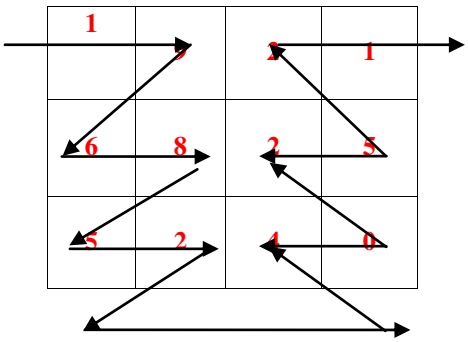
ALGORITHM:

Step 1: Get the input from user.
Eg: IP address – 192.168.255.240 & Time - 22 :46.
Step 2: Arrange the input in N x N matrix.

1	9	2	1
6	8	2	5
5	2	4	0
2	2	4	6

Table 2: 4X4 Matrix for Input

Step 3: Apply the Scan pattern on the matrix to permutate the matrix values.
Eg: Applying 'd' Scan Pattern on the input matrix.



2	2	4	6

Table 3: Applying Scan Pattern

Step 4:

Encrypt(IP; T; N)
Inputs: IP address IP , Time T, Matrix size N × N (N = 4).
Output: Hexa Decimal values H.
{
//get IP and T in an array named as input[]
for(condition){
for(condition){
inputmatrix[][]=input[];//convert 1-D array into 2D array
}}
for(condition){
for(condition){
//permutate input matrix using Scan path until all the positions are visited exactly once.
}}
//read 2 digits from a permutated matrix and convert it into hexa decimal format. Repeat the process until all the values are read from the matrix
}

Every packet is authenticated with a signature. The signature is registered in three nodes. It is a register of packets passing to/fro.

The first node(sender) sends the message with a signature to the destination. Every intermediate node will check the signature which identifies the original set of packets and no attack can be made in between. Every packet with the signature is considered to be a legitimate packet. Every node confirms with the previous and succeeding node about the presence of the signature in each packet.Without the signature, the packets are discarded for security reasons. It involves changes in the TWO PHASE COMMIT protocol.Number of verifications may seem to impose a stress over network performance yet, it can be developed only after simulated results are obtained. The generated signature is shown in the following Figure 2.

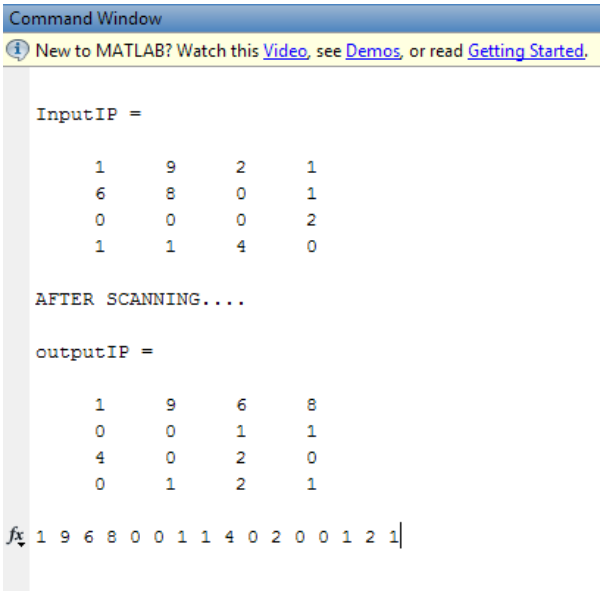


Figure 2: Shuffled Source IP in Packet Headers

A signature would follow the proposed fragments signature algorithm, generating a signature of a random pattern to reshuffle the contents of the matrix. The pattern will be decided upon the detection of an attacker within the network.

Nodes Communication within an internal organisation

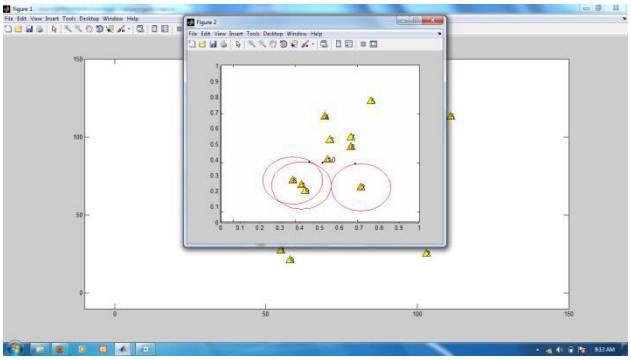


Figure 3: Formation of Clusters and Appointing Cluster Head

The formation of clusters depends on the strength of batteries and the distance with the accommodating nodes. The Figure 3 shows well formed clusters and the appointed cluster heads with respect to the distance in between and here the battery power is assumed to be high during the times of derivation.
And the following figure 4 shows how the packets are transmitted between the nodes.

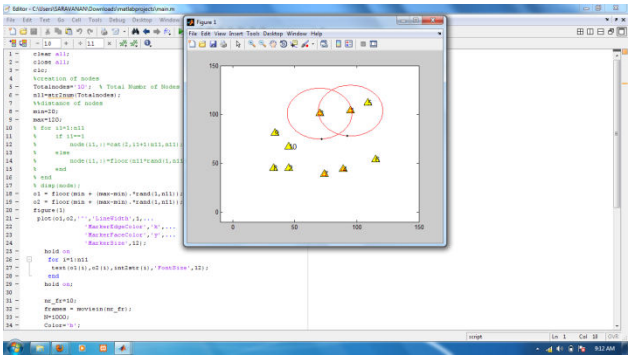


Figure 4: Communication between nodes

RESULTS AND DISCUSSIONS

The energy utilization is estimated with the calculation and transfer of additional metrics for security purpose. The energy has been used at a higher rate resulting in reduction of the sensors lifetime.

The resister would have to maintain the entries of almost all the nodes in the cluster and they have to be cross verified at times of peak traffic, low delivery rate and high transmission rate. The future work includes steps to traceback the attacker with the information updated and timestamps of the intermediate routers or nodes.

REFERENCES

[1] C. Schleher, Electronic Warfare in the Information Age. Artech House, 1999.

[2] R. Mallik, R. Scholtz, and G. Papavassilopoulos, “Analysis of an on-off jamming situation as a dynamic game," IEEE Trans. Commun., vol. 48, no. 8, pp. 1360-1373, Aug. 2000.

[3] A. D. Wood and J. A. Stankovic, “Denial of service in sensor networks," IEEE Comput., vol. 35, no. 10, pp. 54-62, 2002.

[4] R. Negi and A. Perrig, “Jamming analysis of MAC protocols," Carnegie Mellon technical memo, 2003.

[5] J. Bellardo and S. Savage, “802.11 denial-of-service attacks: real vulnerabilities and practical solutions," in Proc. USENIX Security Symp., pp. 15-28, 2003.

[6] A. Wood, J. Stankovic, and S. Son. “JAM: a jammed-area mapping service for sensor networks," in Proc. IEEE Real-Time Syst. Symp., pp. 286-297, 2003.

[7] G. Noubir and G. Lin, “Low-power DoS attacks in data wireless LANs and countermeasures," SIGMOBILE Mob. Comput. Commun. Rev., vol. 7, no. 3, pp. 29-30, 2003.

[8] J. M. McCune, E. Shi, A. Perrig, and M. K. Reiter, “Detection of denial- of-message attacks on sensor network broadcasts," in Proc. IEEE Symp. Security Privacy, 2005.

[9] W. Xu et al., “The feasibility of launching and detecting jamming attacks in wireless networks," in Proc. ACM Int’l. Symp. Mobile Ad Hoc Netw. Comput., 2005, pp. 46-57.

[10] W. Xu, T. Wood, W. Trappe, and Y. Zhang, “Channel surfing and spatial retreats: defenses against wireless denial of service," in Proc. ACM Workshop Wireless Security, pp. 80-89, 2004.

[11] M. Li, I. Koutsopoulos, and R. Poovendran, “Optimal jamming attacks and network defense policies in wireless sensor networks," in Proc. IEEE INFOCOM, May 2007.

[12] A. D. Wood, J. A. Stankovic, and G. Zhou, “DEEJAM:defeating energy- efficient jamming in IEEE 802.15.4-based wireless networks," in Proc. ACM SECON, 2007.

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

[14] J. T. Chiang and Y. C. Hu, “Cross-layer jamming detection and mitigation in wireless broadcast networks," in Proc. ACM MobiCom, 2007.

[15] X. Liu, R. Rajaraman, G. Noubir, B. Thapa, C. King, and E. Bayrak- taroglu, “On the performance of IEEE 802.11 under jamming," in Proc. IEEE INFOCOM, Apr. 2008.

[16] E. N. Gilbert, “Random plane networks," SIAM J., vol. 9, pp. 533-543, 1961.

[17] R. Meester and R. Roy, Continuum Percolation. Cambridge University Press, 1996.

[18] T. K. Philips, S. S. Panwar, and A. N. Tantawi, “Connectivity properties of a packet radio network model," IEEE Trans. Inf. Theory, vol. 35, pp. 1044-1047, Sep. 1989.

[19] O. Dousse, P. Thiran, and M. Hasler, “Connectivity in ad-hoc and hybrid networks," in Proc. IEEE INFOCOM, June 2002.

[20] M. D. Penrose, “Euclidean minimal spanning trees and continuum percolation in high dimensions," preprint.

[21] N. Dunford and J. T. Schwartz, Linear Operators, Part I, General Theory. Wiley-Interscience, 1988.

[22] B. Otis, Y. H. Chee, R. Lu, N. M. Pletcher, and J. M. Rabaey, “An ultra- low power MEMS-based two-channel transceiver for wireless sensor networks," in Proc. IEEE Symp. VLSI Circuits, June 2004.

[23] J. Weldon, K. Jensen, and A. Zettl, “Nanomechanical radio transmitter," Phys. Stat. Sol. (b) vol. 245, no. 10, pp. 2323-2325, 2008.2324 IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, VOL. 10, NO. 7, JULY 2011