International Journal of Trend in Scientific Research and Development (IJTSRD)
Volume: 3 | Issue: 2 | Jan-Feb 2019 Available Online: www.ijtsrd.com e-ISSN: 2456 - 6470

# Security using Location Based Key (LBK) System for Effective Multipath Attack and Protection for Location Discrimination in Wireless Sensor Systems

**Dr. G. Karpaga Rajesh M.E., Ph.D[1], Vaishnu Priya. R[2], Kaviya R[2], Jaya Divya Aj[2]**

[1]Assistant Professor, [2]PG Student, Department of Communication Systems,
Government College of Engineering, Tirunelveli, Tamil Nadu, India

**ABSTRACT**
To obtain secured communication in Wireless Sensor Systems (WSS), a secret shared keys is created between sensor nodes and neighboring nodes. The shortest path is found by using Dijkstra's Algorithm. By the use of this algorithm the energy consumption will be reduced. In this paper, location based key for WSS, with proper attention over the insider attacks is proposed. After reviewing and analysing present key management systems, Location Based Key (LBK) management is selected. To deal with the communication interference problem in LBK, a new key revision technique that involves grid-based location information is devised. Furthermore, a key renew and cancellation processes is constructed to withstand inside attackers in OFDM antenna. For analysis, a accurate simulation is conducted and proved that can increases connectivity and decreases the compromise ratio when the least possible number of common keys needed for key establishment is high.

***KEYWORDS****: Dijkstra's Algorithm, Location Based Key (LBK), Multipath Attacks, Security, Wireless Sensor Systems*

## 1. INTRODUCTION

The Internet was changed life for most people in the last decade. Today most of the new TV sets are Internet capable tries to incorporates most electronic device in the near future. One of the permissive technologies to access and use even the smallest device are Wireless Sensor Systems (WSS). A sensor network have a interval from some rooms to an area of certain square miles in size and so the number of sensor can ranges from a section of nodes to hundreds or thousands. Sensing buildup on the application, many sensors or actuators are available. Battery is used as a power supply. The low cost requirements result in highly constrained resources on a sensor node.

### 1.1 WIRELESS SENSOR SYSTEM

Wireless sensor systems were created in late 1990s.They were made possible by industry scale of small microcontrollers (MCUs) and especially radio interfaces, the two most important building blocks of sensor systems. The early sensor nodes showed the feasibility in 2000. The first widely used platform that also was commercially available was the Mica2, from 2002 and after that around 2004 Telos, TelosB/Tmote and mica were developed.

A Wireless Sensor System (WSS) is a wirelessly connected network of sensor nodes. If the sensor system is only built out of one hardware, then it is called a homogeneous Wireless Sensor Systems, if different platforms are employed it is called a heterogeneous Wireless Sensor Systems. A sensor system can contain static and mobile nodes.

A Wireless Sensor Activator Systems (WSAS**)** is a wireless sensor system, where sensor nodes not only can sense, but also activate. It is also known as wireless actor system. Here they are designed to support not only sensing nodes but also capable of actuation. A Wireless Sensor System Application (WSS Application) describes the overall scenario and specific goals that the application is meant to achieve. To reach the goals an application may be divided into smaller, separates task.

### 1.2 SECURITY

Supporting the basic functionality of executing multiple concurrent applications is handled by the operating scheme. Security is the main analyse in commercial deployments of WSNs. This ensures the confidentiality of exchanged data and prevents malicious nodes from unauthorized joining an arbitrary group. Scoping also provides the ability to hierarchically structure groups and subgroups and enable security measures.

### 1.3 OBJECTIVE

- To obtain security in wireless sensor systems by the use of location based key management.
- To solve the communication interfering problem in LBK using grid based position information.

### 1.4 LOCATION BASED KEY

Location based keys are used for designing security system for sensor networks. Node-to-node authentication is produced based on location based keys, and the establishment of duo wise keys among neighboring nodes is promoted. Location Based Services (LBS) can be approached from a collection of mobile devices to earn value added information related to the user's location. Location based key is used to provide security in the communication networking systems.

## 2. LITERATURE SURVEY

### 2.1 ROBUST LOCATION DISTINCTION USING TEMPORAL LINK SIGNATURES

The receiver will be able to determine when the location of a transmitter has changed. It is necessary for the conservation of energy in wireless sensor systems, to determine replication attacks in wireless network security. In this paper temporal link signature is proposed to merely determine the link between the transmitter and receiver. This will lower the fake alarm estimate and increases the detection rate.

### 2.2 ADVANCING WIRELESS LINK SIGNATURES FOR LOCATION DISTINCTION

Location distinction is used to determine when the device has interchanged its position. In this multi-tonal probes channel gain and channel impulse response are compared. Then, the uses of these methods is mixed to establish a new link analysis complex temporal signature. This method operates more effective when compared with the existing methods. This will reduce the false alarms probability because of sequential variations of linkage signatures.

### 2.3 CHANNEL BASED DETECTION OF SYBIL ATTACKS IN WIRELESS NETWORKS

Wireless networks are highly sensitive to Sybil attacks, where a malicious node claims a number of integrities and drains system resources. Hence an improved physical-layer authentication method to determine Sybil attacks is proposed. This method can be easily realized with low overhead when compared with existing methods, either individually or combined with other physical-layer security schemes. This estimation determines different system parameters, such as bandwidth, signal power, number of total clients, number of Sybil clients and number of access points.

### 2.4 ENHANCED WIRELESS CHANNEL AUTHENTICATION USING TIME-SYNCHED LINK SIGNATURES

Wireless linkage signature is a visible level validation scheme, will provide wireless channel authentication. In the existing methods mimicry attack was described. A time synched linkage signature is proposed to prevent the mimicry attack, by combining cryptographic security and time factor into usual wireless linkage signatures is suggested.

### 2.5 SECURING WIRELESS SYSTEMS VIA LOWER LAYER ENFORCEMENTS

Cryptographic security schemes are important to overcome the issues in securing wireless networks. This paper suggest to apply the radio channel to develops new authentication and confidentiality that operate at the physical layer and used to promotes cross-layer security standards. Especially, two channel probing schemes are used to find the accuracy of a transmitter for authentication services

## 3. EXISTING METHOD

In wireless system, location distinction desires to determine location changes or helps verification of wireless users. To attain location distinction, recent analysis has concentrated on analyzing the wireless dimensional uncorrelation property mediums. However, a new attack across all present location distinction schemes that are designed on the basis of spatial uncorrelation property of wireless mediums is detected. To resist against this attack, a technique which uses an antenna to spot the fake channel characteristics is proposed.

A WSS model is consist of a Base Spot (BS), a Chunk Head (CH), Anchor Nodes (ANs), and Sensor Nodule (SNs). An SN finds the near node, senses and collects information, and sends during a hop-by-hop model to a CH. An AN transmits different nonces to SNs to a power level. The SN develops a duo wise key applying the nonces received from the AN.

Figure 1 shows the network model of wireless sensor system.

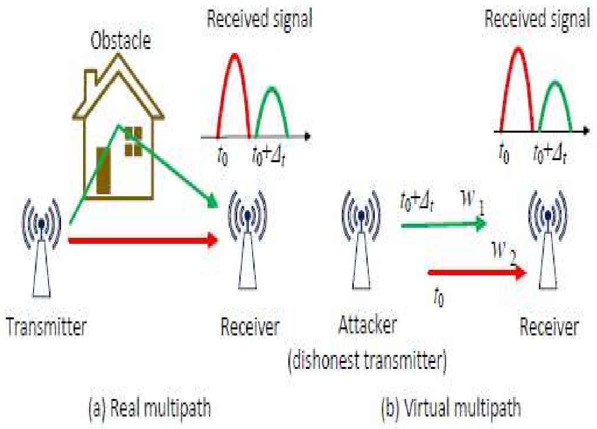


**Figure 1:** Network model

An insider attack is more critical than an outsider attack because it bypasses authentication and authorization and drops critical packets. Various types of insider attacks include modification, misrouting, dropping, and package drops. The package drop attack is particularly difficult to detect. Package drop attacks are divide into black hole attack, a gray hole attack, or an on–off attack. Because of the characteristics of gray hole and on–off attacks, they are more crucial to determine than black hole attacks. Here, the objectives is to provide security against package drop attackers and other internal attackers.

This scheme presents the key establishment process using ANs based on LBK. This scheme is named as LBK. LBK has two steps. First, SNs generate a communication key to manage keys, and then, the keys are updated to secure the network against insider threats. Key revision aspect from a near node and manage the key establishment process using grid information The situation where the SN does not deploy in the assigned grid position is considered. The present key management systems using a grid for WSNs utilize a grid as a key ring or an identifier, which uniquely identifies an SN. One of the conditions among the schemes is that an SN should be deployed in an assigned grid. Through this simulation, confirm that LBK has high connectivity and a low compromise ratio, that improves stability and security.

### 3.1 DEFENDING AGAINST EFFECTIVE MULTIPATH ATTACK

Effective multipath attackers are capable to create the receiver admit any channel features that the attacker accepts. At the receiver, it appears that no idea to tell whether the signal goes through real or virtual multipath situation. The attacker will bring a second transmitter to confuse the receiver. Attacker's second transmitter is referred as the attacker's helper.

Hence, existing location distinction methods built upon distinguishing locations from channel characteristics will be easily defeated by virtual multipath attacks. Let the receiver use two different training sequences x1 and x2 to measure the channel impulse response alternatively. Assume that the receiver uses x1 to measure the medium from the first transmission, and uses x2 to measure the medium from the second transmission. For both transmissions, at the receiver, the virtual channel created by a malicious transmitter (i.e., the attacker) can result in the same estimated channel impulse responses (equal to the one chosen by the attacker). Figure 2 shows the defense against effective multipath attack.

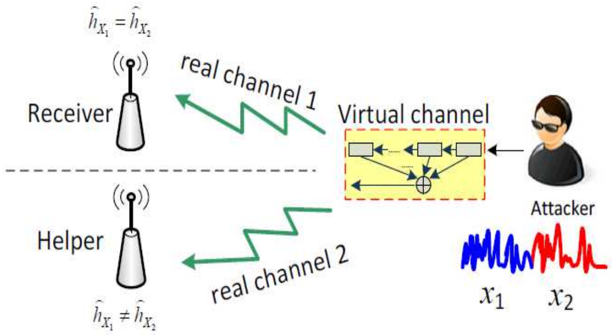


**Figure 2:** Defense Against Effective Multipath Attack

### DRAWBACKS

- Energy consumption is high.
- Slow response time.
- High SNR.
- Insider and outsider attacks not clearly solved.

## 4. PROPOSED SYSTEM

Communication between two unclustered nodes is detecting through intermediate nodes. This will be applicable in habitat monitoring, disaster relief and target tracking. A number of applications need simple and cumulative function to be noted. Clustering shows collection and reduces data transmissions. Nodes divided in fundamental group according to different rules. Nodes present in a group will implement different functions from other nodes and these group of node cluster choosing the CH (cluster head ) member head of the cluster and those node will simply communicate with their CH.

The work of CH, to send the all aggregative data to central base station or (main central head) CHs. The clustering objectives allows aggregation the limits data transmission can facilitate the resources reusability of CH and entry nodes will form a basic backbone for inter cluster routing . Each node use a minimal spanning tree and localized minimal spanning tree is calculated by Dijkstra's algorithm.

In this algorithm different node depends on locally best decision each and every node have its own information and they exchange its own loop neighborhood. The location based key is used to increase the security of the system. The Dijkstra's algorithm is employed to calculate the shortened path between the source and destination node. Data acquisition is a method of sampling data signals which evaluate actual physical conditions and changing the end samples into digital codes will be employed by a computer. Figure 3 shows the Data Acquisition model.

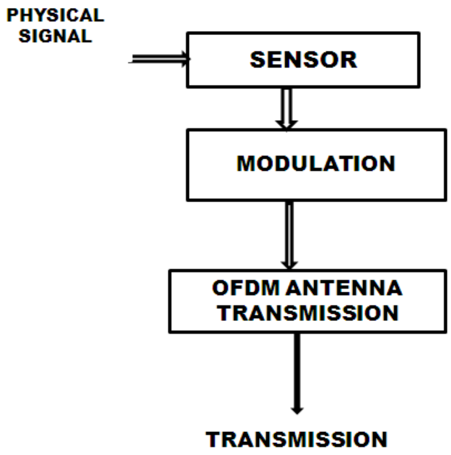


**Figure 3:** Data Acquisition Model

Data acquisition systems consists of

- Sensors are employed to convert physical signals into electrical signals.
- Using Signal conditioning circuitry sensor signals are changed into the form then it will be converted to a digital signals.
- Analog-to-digital converters are used to convert conditioned sensor signals to digital codes.

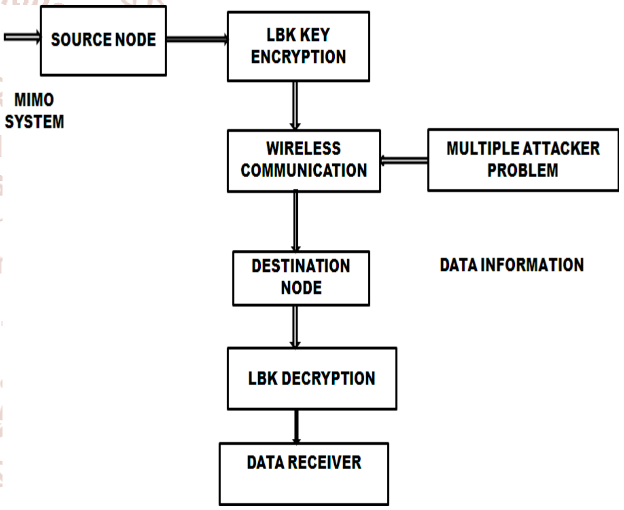


**Figure 4:** Proposed System Block Diagram

The proposed system consist of LBK Encryption and LBK Decryption. Figure 4 shows the proposed system block diagram. In the initializing if the all node can't define the path then shortest path SN (v) =∞ If the nodes will labelled then queue will be maintain with priority wise (q) in this condition start node SN (v) =0 it means current distance is small. These are symbols which are used in Dijkstra's model m= no of network node V is sending node w is receiving node k is transmission radius u relay node cos( ɵ)[i][j] is distance between i and j. By using Dijkastra algorithm the problem of maximum distance is solved. By using model suggest given the following the algorithm:

1. Initialization: number=0 , distance =+ ve infinity, set l[i] =0 Where i= (0,1,2,3-m);.
2. If cos( ɵ) [v] [i]< k, then Setl [i]=1,(i= 0,1,2,------m); Cos [i][j] distance between node i and j.
3. If Set [w] =1 ,then distance =cos( ɵ) [v] [w] ; else go to step 4;.

4. For all I belongs to {set l [i] = 1} , u [ number] =1 ,set l[j] =1 when j belongs to { cos( ɵ ) [u [number] ][j] < k } for all j= 0.1.2------n);.
5. If set[w] ≠ 1, then num++, repeat step otherwise record the distance that fulfils set[w]=1, Distance of number = cos( ɵ) [v] [u (0)]+∑ ( )[ ][ ( )] ( ) [()].

This algorithm give the shortest path and conducting of simulation of a network given k=5 set. Through the cluster structure the lifetime of network is easily improved and easily decreases traffic of the network. Minimum spanning Tree and localized Minimum spanning Tree calculated with Dijkstra algorithm is used.

Each node transfers its neighborhood information with its entire one loop neighborhood information. Any node with two unlinked neighbors becomes a dominator. In open neighbor set R (v), Minimal Spanning Tree (MST) and Localized Minimum Spanning Tree (LMST) is calculated with not make use of varients, eg., ID nodes. Every sensor nodes possess multiple power levels, chooses CHs in line with node net energy and degree of node.

### 4.1 KEY GENERATION

In addition to its LBK, each node, say A, should possess a location-based key, or LBK for short, LKA = kH1(posA) = kH1(xA k yA) ∈ G1, where "k" denotes the concatenation of messages. Mobile robots are equipped with both the system specifications and the system master-key so that they can generates LBKs for individual nodes. Mobile robots will protected and programmed so that they should be able to eliminate the system-master key 'k' completely after the key formation stage. Mobile robots cannot simply send LBKs in plaintext to individual nodes and they are required to execute the following protocol:

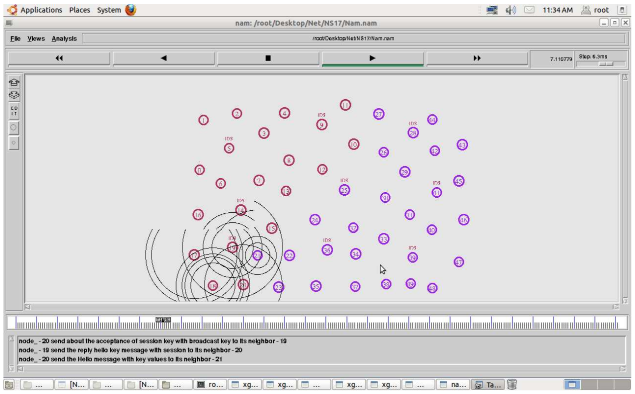
T1 → A : "helloLBK" (broadcast);
A → T1 : IDA (unicast);
T1 → A : {IDA, posA, LKA}IKA (unicast),

where T1 denotes a robot and A is one of the nodes to be initialized. In the above protocol, T1 first broadcasts a special "helloLBK" word to declare its existence. If seeing such a message and still uninitialized, node A responds with its identifier IDA by unicast. Then T1 proceeds to determine posA and generates IKA= k(IDA) and LKA=kH1(posA).

After that, T1 encrypts IDA, posA, and LKA with the encryption key IKA using any efficient secret-key function such as RC5 and unicasts the ciphertext to node A. Node A can then decrypt the ciphertext with the pre-loaded IKA. Note that, in the third step above, T1 can also pack together the responses for several nodes and broadcast them in one message to the target sensors that reduce the communication.

## 5. RESULTS AND DISCUSSION

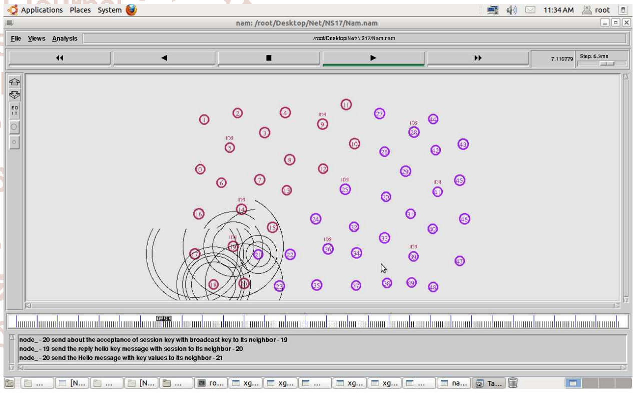
The proposed work is simulated through Network Simulator in TCL language format. The present key management schemes employing a grid for WSNs utilize a grid as a key ring or an identifier, which uniquely identifies an SN. One of the conditions among the schemes is that an SN should be deployed in an assigned grid. A sensor in a sensing network is set to collects sensory information and interacting with other linked nodes within the network. When a node is captured, a secure link is broken because the communication key is derived from a few common keys. In this project created rectangular node using 50 sensor nodes and one anchor node. The dijikstra algorithm is employed to locate the shortened path from supply to the destination nodes. Figure 5 shows the source node creations. Wireless data transmissions are achieved with the help of mobile stations. These mobile stations are called Sensor nodes. In this energy of the nodes are assigned.



node_ - 20 send about the acceptance of session key with broadcast key to its neighbor - 19
node_ - 19 send the reply hello key message with session to its neighbor - 20
node_ - 20 send the Hello message with key values to its neighbor - 21

**Figure 5:** Sensor node creations

Anchor nodes are those sensing element nodes whose location is recognized. These nodes are used to detect the position of sensor nodes whose location is unidentified. Figure 6 shows the anchor node formation between source node and anchor node.



node_ - 20 send about the acceptance of session key with broadcast key to its neighbor - 19
node_ - 19 send the reply hello key message with session to its neighbor - 20
node_ - 20 send the Hello message with key values to its neighbor - 21

**Figure 6:** Anchor node formations

In this project main aim is to lower the energy consumption. The datas are transmitted through variety of mobile stations. It is important to decrease the energy consumption in order to calculate the next node with less distance. Figure 7 shows the packet comparison of the systems.

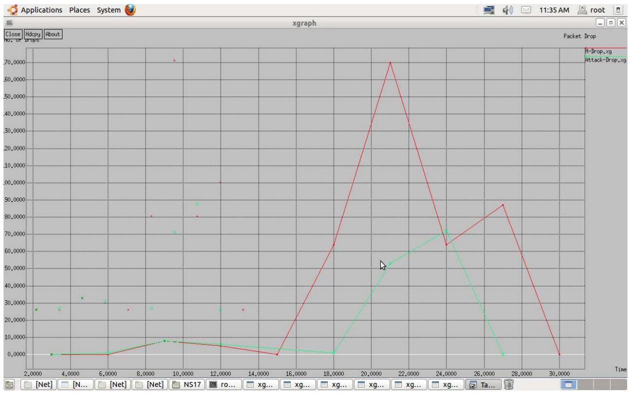


**Figure 7:** Packet drop comparison

In order to diminish the attacker problems we have use protection keys for increasing the system security. The location based key is used to rise the security safety of the system. In data communication, network throughput is the capacity of data carried strongly from one node to another node in a given duration of time. Figure 8 shows the throughput comparison between various algorithm.

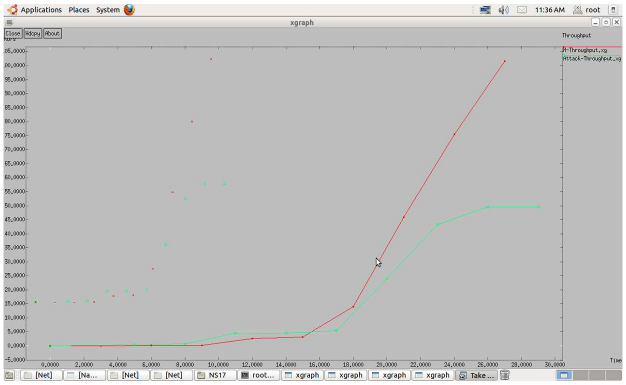


**Figure 8:** Throughput comparison

## 6. CONCLUSION AND FUTURE SCOPE

### 6.1 CONCLUSION

In this project, LBK scheme is presented, which is an improved version of the key management scheme. Key revisions by incorporating the use of grid information into the previous dividing method is added, and key generation by combining the grid information is suggested. The problem of inadequate numbers of nonces that can appear due to the communication interference is solved. In this paper key establishment and key revocation, along with packet drop attack among alternative insider attacks are examined. Through this simulation, confirm that LBK has high connectivity and low compromise, thus improves strength and security. The Dijkstra algorithm used for locating the shortened path between source and anchor node. This algorithm also reduces the energy consumption.

### 6.2 FUTURE SCOPE

We can use modified Dijkstra's algorithm for increasing the speed of the shortest path calculation. Instead of Location Based Key, Layered Location Based Key to increase the security.

## REFERENCES

[1] John Bethencourt, Amit Sahai, and Brent Waters, "Ciphertext-policy attribute based encryption," in IEEE Symposium on Security and Privacy, SP 2007, pages 321–334, Berkeley, CA, June 2007.

[2] J. Zhang, M. H. Firooz, N. Patwari, and S. K. Kasera, "Advancing wireless link signatures for location distinction," in Proc. of ACM MobiCom '08, September 2008, pp. 26–37.

[3] K. S. Shanmugan and A. M. Breipohl, "Random signals: detection, estimation, and data analysis," in Wiley, May 1988.

[4] L. Xiao, L. J. Greenstein, N. B. Mandayam, and W. Trappe, "Channel based detection of sybil attacks in wireless networks," IEEE Trans. Information Forensics and Security, vol. 4, no. 3, pp. 492 – 503, 2009.

[5] M. Edman, A. Kiayias, and B. Yener, "On passive inference attacks against physical-layer key extraction," in Proceedings of the Fourth European Workshop on System Security, 2011.

[6] N. Patwari and S. K. Kasera, "Robust location distinction using temporal link signatures," in Proc. of ACM MobiCom '07, September 2007, pp. 111–122.

[7] O. Edfors, M. Sandell, J. J. V. de Beek, S. K. Wilson, and P. O. Borjesson, "OFDM channel estimation by singular value decomposition," IEEE Trans. Communications, vol. 46, no. 7, pp. 931 – 939, 1998.

[8] Xiangqian Chen, K. Makki, Kang Yen, and N. Pissinou, "Sensor network security: a survey," Communications Surveys Tutorials, IEEE, 11(2):52 –73, April 2009.

[9] X. He, H. Dai, W. Shen, and P. Ning, "Is link signature dependable for wireless security?" in Proc. of IEEE INFOCOM '13, April 2013.

[10] Y. Liu and P. Ning, "Enhanced wireless channel authentication using time-synched link signature," in Proc. of IEEE INFOCOM '12, March 2012.

[11] Y. Liu and P. Ning, "Poster: Mimicry attacks against wireless link signature," in Proc. of ACM CCS'11, 2011.

[12] Y. Liu, P. Ning, and H. Dai, "Authenticating primary users' signals in cognitive radio networks via integrated cryptographic and wireless link signatures," in Proc. of IEEE S&P '10, May 2010, pp. 286–301.

[13] Z. Li, W. Xu, R. Miller, and W. Trappe, "Securing wireless systems via lower layer enforcements," in Proc. of ACM WiSe '06, September 2006, pp. 33–42.