ISSN: 0974-5572

IJCTA

International Journal of
CONTROL THEORY
AND APPLICATIONS

UGC APPROVED JOURNAL

ज्ञान-विज्ञान विमुक्तये

INTERNATIONAL SCIENCE PRESS
Gurgaon, Haryana (India)

International Journal of Control Theory and Applications

ISSN : 0974-5572

© International Science Press

Volume 10 • Number 36 • 2017

Prevention of Intentional Interference Attacks in Wireless Networks (PIIA)

K. Sivakumar[a] **and K.A. Parthasarathy**[b]

[a]*Research Scholar, Department of Computer Science and Engineering, St. Peter's University, Chennai, India. Email: sivakumarstpeters@gmail.com*
[b]*Principle, Department of Computer Science and Engineering, Akshaya College of Engineering, Kancheepuram, India*

Abstract: The wireless medium is built upon shared medium; hence it is vulnerable to intentional interference attacks, typically referred to as jamming. Intentional interference with wireless transmissions can be used as a launch pad for Denial-of-Service (DoS) attacks on wireless network. Jamming referred as external threat model and detection of these attacks is not so difficult. However, adversaries with internal knowledge of network protocol specifications and secrets can instigate low-effort jamming attacks that are difficult to detect and counter. The problem of selective jamming attacks on routing is addressed in the proposed method. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. The selective jamming in terms of network performance degradation and adversary effort by presenting a selective attack on routing is illustrated. The selective jamming attacks in wireless data transmissions can be launched by performing real-time packet classification at the physical layer.

To reduce these attacks a scheme is proposed, that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. The computational cost and communication overhead are analyzed using the simulation tool.

Keywords: Wireless Networks, Selective Jamming, Denial-of-Service, routing, Packet Classification.

1. INTRODUCTION

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. A malicious node can continually transmit a radio signal in order to block any legitimate access to the medium and/or interfere with reception. This act is called jamming and the malicious nodes are referred to as jammers [1].

While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses.

Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high-power interference signals. A jammer can interfere with normal communications between two legitimate communicators in two ways: preventing the sender from sending out packets, or preventing the receiver from receiving packets. Hence, we use the resulting Packet Send Ratio (PSR) and Packet Delivery Ratio (PDR) to measure the effectiveness of a jammer.

The remainder of the paper is organized as follows. The previous jammers methods described in Section II. Section III presents the Prevention of Intentional Interference Attacks In Wireless Networks (PIIA). Section IV discusses about the simulation results. Finally, Section V presents conclusion.

This rest of this paper is organized as follows. Section 2 describes the related work. In Section 3, proposed method (i.e.) Routing Promotion by Intermediate Relays (RPIR) for Successful Mobile Ad-hoc Networks Communication is presented. The simulation results and comparative performance analysis is given in section 4. The conclusion is presented in Section 5.

2. RELATED WORKS

The jammers cause the effective network activity factor and hence the interference among the BSs to be doubled. In particular, a non-trivial behavior is seen that indicates that the number of jammers required to attack the wireless network must scale with the BS density only until a certain value beyond which it decreases [2]. Wormhole Attack Detection Algorithms [3] used to detect wormholes and show its correctness rigorously. Distributed detection Algorithm against Wormhole coding systems (DAWN) exploring the change of the flow directions of the innovative packets. DAWN guarantees a good lower bound of successful detection rate. It finds that the robustness depends on the node density in the network, and proves a necessary condition to achieve collusion-resistance.

Efficient Cooperative Watchdog Monitoring method [4] efficiently detect pollution attacks in a lossy wireless environment. This method cooperatively to share the packet information, reduce the overhead to normal transmission nodes, and rather than retransmitting all lost packets among watchdogs. Watchdogs use randomly generated Vander monde hashes to detect corrupted packets and capable of detecting successive colluded adversaries. In addition, it achieves low computational complexity and communication overhead.

Secrecy Rate Optimization for Secure multicasting Scheme [5] transmitter broadcasts the similar information to a group of legitimate users in the presence of eavesdroppers. This scheme functions are minimized the power and maximized the secrecy rate. These jammers charge the transmitter for their jamming services based on the amount of the interference caused to the eavesdroppers. Stackelberg equilibrium is derived to maximize the revenues of both the transmitter and the private jammers. Source-Based Jamming (SBJ) scheme [6] is proposed to improve the secrecy performance of un-trusted relay networks. In this scheme, the direct link is utilized in secure transmission and provides flexibility cooperation. The SBJ scheme is used to maximize the average secrecy capacity, from which the power of the source and relay nodes and the power of the information and jamming signals are optimally allocated.

Secure Communication approaches [7] establish reliable communication and data confidentiality directly at the physical layer of a communication network by taking the properties of the noisy channel into account leading to unconditional security regardless of the computational capabilities of eavesdroppers. The provision of accurate channel state information is a major challenge particularly in wireless communication systems, especially information about the channels to eavesdroppers. In addition, there might be malevolent adversaries who jam or influence the channel of the legitimate users. Authentication framework with Conditional Privacy-preservation and Non-repudiation (ACPN) [8] introduced the public-key cryptography (PKC) to the pseudonym generation that ensures legitimate third parties to achieve the non-repudiation of vehicles by obtaining vehicles' real IDs. The self-generated PKC-based pseudonyms are also used as identifiers instead of vehicle IDs for the privacy-preserving authentication. The ID-based signature (IBS) scheme and the ID-based online/offline signature (IBOOS) scheme are used to authentication between the Road Side Units (RSUs) and vehicles, and the authentication among vehicles, respectively.

Ant Colony Optimization [9] analyzed with the application of shortest path algorithm in Virtual Private Network. Distributed jammer network (DJN) [10] that analyze the impact of jammer on the connectivity of the target network, and provide lower and upper bounds for the percolation of the target network. It provides the scaling analysis of the jamming performance in relation to the jammer node density with the power density constraint. Anti-jamming Interference Alignment (IA) [11] is an effective method for battling adversarial jammers for IA networks. An anti-jamming opportunistic IA (OIA) scheme with wireless EH (Energy Harvesting) that optimizes the transmission rate and minimize the energy consumption in the networks. This scheme used to make the anti-jamming IA network feasible. The transmit power and power partition coefficient are jointly optimized to minimize the total transmit power of the OIA network. This scheme reduces the computational complexity of the joint optimization. An anti-jamming channel hopping approaches without pre-shared secrets have gained more and more research interests. An anti-jamming channel hopping scheme, Sec-CH. Sec-CH has bounded time to rendezvous and can work without role pre-assignment [12].

Security-Reliability Tradeoff for Friendly Jammer Assisted User-Pair Selection explored the physical-layer security in a wireless network consisting of multiple user pairs in the face of multiple eavesdroppers that are deployed by an adversary for tapping the confidential transmissions of the user pairs deliberately. A friendly jammer-assisted user-pair selection (FJaUPS) scheme used to improve the security-reliability tradeoff (SRT). Friendly jammer is used to transmit the artificial noise that is specially designed onto the null space of the main channel for the sake of not interfering with the destination. The impacts of the friendly jammer on the legitimate user transmissions and eavesdroppers are taken into account for evaluating the wireless SRT performance that are quantified by the so-called self-interfering factor and jamming factor, respectively [13].

Packet-Hiding Methods (PHM) [14] addresses the problem of Selective Jamming Attacks in the network. A sophisticated adversary is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of high importance are targeted. This scheme using the cryptographic mechanisms with PHY-layer attributes. It achieves strong security properties, with minimal impact on the network performance. However, this method creates additional overhead in the network.

3. PREVENTION OF INTENTIONAL INTERFERENCE ATTACKS

Securing the sensor network and detecting the radio interference attacks is a challenging task in sensor network due to the availability of low resources associated with the sensor nodes. The problem of jamming under the internal threat model is addressed here. The adversary has the knowledge of network secrets and implementation of network protocol details. Hence the adversary can easily launch the attack by targeting specified messages 'high importance' by implementing selective jamming attack on routing and packet transmission.

By estimating the level of signal strength and packet delivery ratio the presence of jamming attack or adversaries can be determined. The Threshold level of signal strength is determined and compared with the actual received signal strength. If the received signal strength is zero or very low in comparing with the threshold level, then this indicates the presence of jammer or adversary node. Jammers may be proactive or reactive. Proactive jamming technique continuously emits radio interference signal in order to jam the node's data transceiver signal.

For every layer in the network stack the implementation details are assumed to be public. Furthermore, the adversary node is capable of compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. Network architectures such as mobile ad hoc, cognitive radio, mesh and wireless sensor networks (WSNs), this internal adversary model is realistic where network devices may operate unattended might be susceptible to physical compromise.

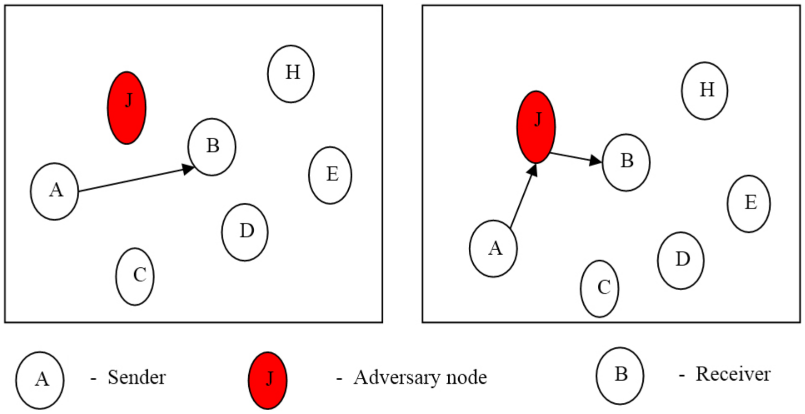

Figure 1: Example Scenario of Proposed Scheme

In this figure A termed as sender node, B termed as receiver node and J acts as adversary node.

2. Reactive Jamming

Reactive jamming is the most power-efficient technique and also the only one that can achieve minimal invasiveness: in reactive jamming, in fact, the interfering signal is selectively emitted only when another specific signal is detected on the channel. The function of reactive jammer stays quiet when the channel is idle, but starts transmitting a radio signal as soon as it senses activity on the channel.

A. **Selective Jamming Attack on Routing:** The sender initiates routing path by generating RREQ with Time to Live (TTL) value equal to one hop. Then the sender expects RREP within the expiry time (time out) and if RREP does not received by the sender, then the sender node extends the TTL value and rebroadcast the route request message and this process continues until the reception of valid RREP. The non reception of RREP indicates the presence of jammer. This jammer generates the jamming signal by sensing the activity of generated RREQ to interfere the communication at the initial stage.

B. **Selective Jamming Attack on Data Transmission:** In wireless networks the data communication is done by sending radio waves from sender to receiver. The frequency of the sending and receiving signals are measured. Once the data is sending from the sender to the receiver then the adversary node present in this range will generate the interference signal with same frequency range of sender's data. Radio frequency jamming is launched during data transmission.

The selective jamming attack is implemented by selecting the packets with high importance. The high importance message can be picked by classifying the message. The adversary node classifies the packets in real time before the completion of packet transmission. Based on the strategy the adversary may select the packets to jam once the packet classification is done.

The adversary's ability of classifying the packet '*m*' is depends on the implementation of blocks includes sender side as well as receiver side. The sender block includes channel encoder, inter-leaver and modulator; receiver block includes channel decoder, de-inter-leaver and de-modulator. The adversary can send the interference signal in any of the blocks because it knows the internal protocol specification and it can able to work even at high transmission speed. It can classify the *m* packets by and necessary redundancy bits are added for protection. The static key is used as security key for the packet '*m*' and providing static encrypting key and static decrypting key for the packet for both sender and receiver would be the intuitive solution for the selective jamming attacks. The '*m*' packet can be encrypted by using cipher-text block C_i.

$$C_{i+1} = E_k(C_i \oplus M_i) \quad i = 1, 2, ..., n \tag{1}$$

where,

E_k – Encrypted key

M_i – packet

The plain text *m* can be recovered using the equation

$$M_i = C_i \oplus D_k(C_{i+1}) \quad i = 1, 2, ..., n \tag{2}$$

where,

D_k – Decrypted Key

The adversary node performs packet classification by exploiting inter-packet timing information to interfere the ongoing packet transmissions. The selective jamming attack can be prevented by using the cipher-text cryptanalysis mechanism. By using this mechanism the characteristics of packet length and inter-packet timing get changed so that the efficiency of selective jamming is reduced. However the signal gets distracted randomly.

4. PERFORMANCE EVALUATION

The performance of the proposed scheme is analyzed by using the Network simulator (NS2). NS2 is a discrete event time driven simulator, which is used to mainly model the network protocols. The NS2 is an open source programming language uses C++ in back-end and OTCL (Object Oriented Tool Command Language) in front-end. The nodes are distributed in the simulation environment. The parameters used for the simulation of the proposed scheme are tabulated in Table 1.

Table 1
Simulation Parameters of PIIA

Parameter	*Value*
Number of nodes	50
Routing scheme	PHM and PIIA
Traffic model	VBR
Simulation Area	1000x1500
Channel	Wireless Channel
Transmission range	250m
Communication Protocol	TCP
Antenna	Omni Antenna

The simulation of the proposed scheme has 50 nodes deployed in the simulation area 1000 × 1500. The nodes are communicated with each other by using the communication protocol Transmission Control Protocol (TCP). The traffic is handled using the Variable Bit Rate (VBR). The radio waves are propagated by using the propagation model two-ray ground. All the nodes receive the signal from all direction by using the Omni directional antenna. The performance of the proposed scheme is evaluated by the parameters packet delivery ratio, packet loss ratio, average delay, throughput and residual energy.

Packet Delivery Rate

Packet Delivery Rate (PDR) is the ratio of the total number of packets successfully delivered to the total packets sent. It is obtained from the equation (3) below.

$$\text{PDR} = \frac{\text{Total Packets Received}}{\text{Total Packets Send}} \tag{3}$$

The Figure 2 shows the PDR of the proposed scheme PIIA is higher than the PDR of the existing method PHM. The greater value of PDR means better performance of the protocol.

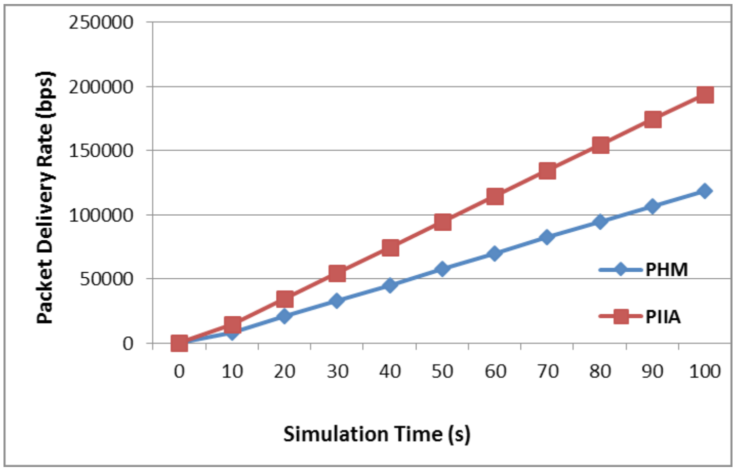

Figure 2: Packet Received Rate

Packet Loss Rate

Packet Loss Rate (PLR) is the ratio of the packets lost to the total packets sent, estimated by the equation (4) below,

$$\text{PLR} = \frac{\text{Total Packets Dropped}}{\text{Total Packets Send}} \tag{4}$$

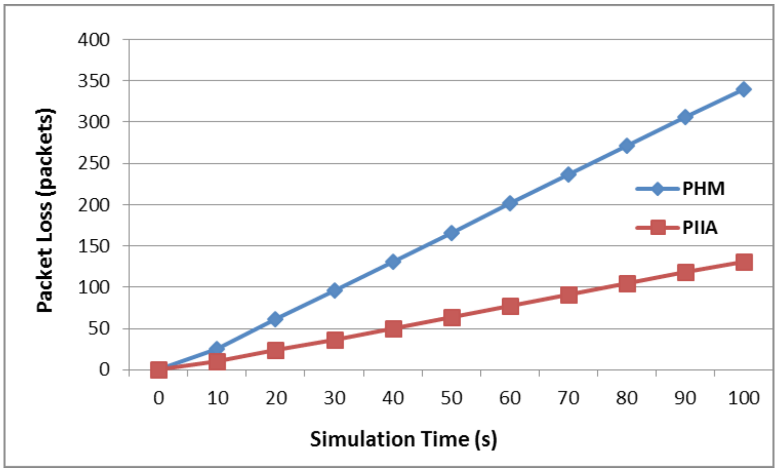

Figure 3: Packet Loss Rate

The PLR of the proposed scheme RPIR is lower than the existing scheme POR in Figure 4. Lower the PLR indicates the higher performance of the network.

Average Delay

Delay is defined as the time difference between the current packets received and the previous packet received. The delay in the network degrades the performance of the network. The average delay is measured by equation 5.

$$\text{Delay} = \frac{\sum_{0}^{n} \text{Pkt Send Time} - \text{Pkt Recvd Time}}{\text{Time}} \tag{5}$$

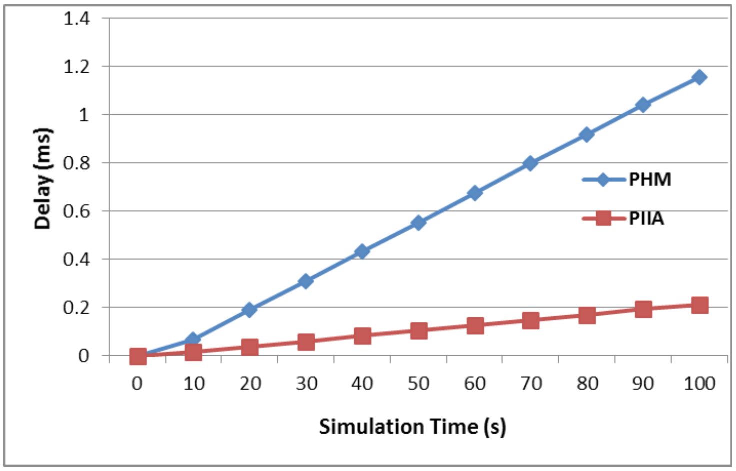

Figure 4: Average delay

Figure 4 shows that the delay value is low for the proposed scheme PIIA than the existing scheme PHM. The minimum value of delay means that higher value of the achievable throughput of the network.

Throughput

Throughput is defined as the rate at data is successfully transmitted for every packet sent. The average throughput is estimated using equation 6.

$$\text{Throughput} = \frac{\sum_{0}^{n} \text{Pkts Received}(n) \times \text{Pkt Size}}{1000} \tag{6}$$

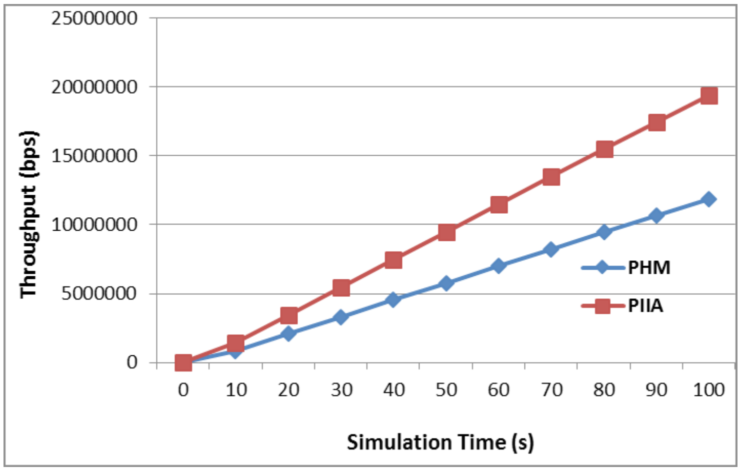

Figure 5: Throughput

Figure 5 shows that the proposed scheme PIIA has greater average throughput when compared to the existing scheme PHM.

Normalized Routing Load

The total packets received contain the sum of the routing packets and the control packets. Figure 6 shows the normalized routing load at number of experiments.

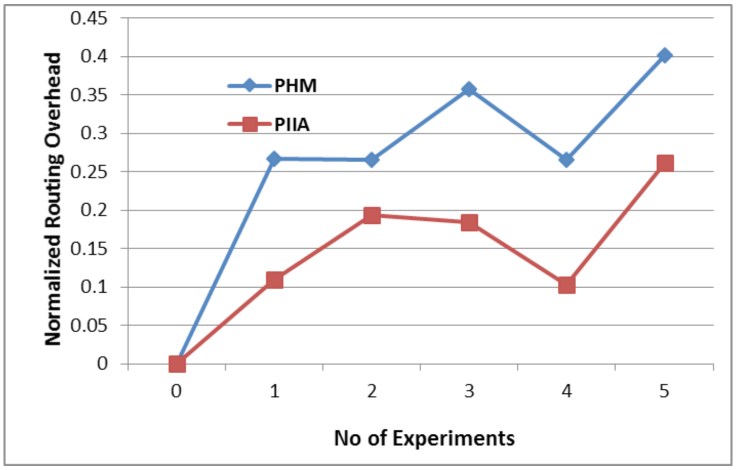

Figure 6: Routing Overhead

The normalized routing loads show that the proposed mechanism performs better than the existing system. PIIA has low overhead when compared to PHM as shown in the above figure. Hence, the ratio of the routing packets to the total received packets implies the difference in overhead observed.

5. CONCLUSION

Problem of selective jamming attacks in wireless networks is addressed and adversaries with internal threat model are taken into important consideration. The selective jamming attacks on routing and selective jamming attack on data transmission are considered in this mechanism and the presence of jammers are considered based on the zero signal strength, packet sent ratio and packet receive ratio. The cipher-text messages using cryptanalysis are proposed to avoid the internal interference occurred in the wireless data transmission. Selective jammer can noticeably impact performance with very low effort is shown in this scheme. However, the jammer is transformed from selective to a random one by applying the key mechanism for data transmission. The efficiency of the results are analysed using the simulation tool and shown.

REFERENCES

[1] Pelechrinis, K., Iliofotou, M., & Krishnamurthy, S. V. “Denial of service attacks in wireless networks: The case of jammers,” IEEE Communications Surveys & Tutorials, Vol. 13, No. 2, pp. 245-257, 2011.

[2] Amuru, S., Dhillon, H., & Buehrer, R. M. “On Jamming Against Wireless Networks,” IEEE Transactions on Wireless Communications, 2016.

[3] Ji, S., Chen, T., & Zhong, S. “Wormhole attack detection algorithms in wireless network coding systems,” *IEEE Transactions on Mobile Computing*, Vol. 14, No. 3, pp. 660-674, 2015.

[4] Lou, X., Yao, H., Tan, C. W., & Wang, J. “VANDER: Efficient Cooperative Watchdog Monitoring for Lossy Wireless Network Coding,” *IEEE Transactions on Vehicular Technology*, Vol. 64, No. 2, pp. 702-713, 2015.

[5] Cumanan, K., Ding, Z., Xu, M., & Poor, H. V. "Secrecy rate optimization for secure multicast communications," IEEE Journal of Selected Topics in Signal Processing, Vol. 10, No. 8, pp. 1417-1432, 2016.

[6] Lv, L., Chen, J., Yang, L., & Kuo, Y. "Improving Physical-Layer Security in Untrusted Relay Networks: Cooperative Jamming and Power Allocation," IET Communications. 2016.

[7] Schaefer, R. F., Boche, H., & Poor, H. V. "Secure communication under channel uncertainty and adversarial attacks," Proceedings of the IEEE, Vol. 103, No. 10, pp. 1796-1813, 2015.

[8] Li, J., Lu, H., & Guizani, M. "ACPN: A Novel Authentication Framework With Conditional Privacy-Preservation And Non-Repudiation for VANETs," IEEE Transactions on Parallel and Distributed Systems, Vol. 26, No. 4, pp. 938-948, 2015.

[9] Chandra, S., Shrivastava, U., Vaish, R., Dixit, S., & Rana, M. "Improved-AntNet: ACO routing algorithm in practice," In *Computer Modelling and Simulation, 2009. UKSIM'09. 11th International Conference on* IEEE, pp. 25-29, 2009.

[10] Huang, H., Ahmed, N., & Karthik, P. "On a new type of denial of service attack in wireless networks: The distributed jammer network," IEEE Transactions on Wireless Communications, Vol. 10, No. 7, pp. 2316-2324, 2011.

[11] Guo, J., Zhao, N., Yu, R., Liu, X., & Leung, V. "Exploiting Adversarial Jamming Signals for Energy Harvesting in Interference Networks," *IEEE Transactions on Wireless Communications*, 2016.