An Improved Packet Hiding Method for Preventing Selective Jamming Attacks in Wireless LAN

Bhoomi Patel
M.E Student
Department of Computer Science & Engineering
Narnarayan Shastri Institute of Technology, Jetalpur, Gujarat, India

Anand Chauhan
Assistant Professor
Department of Computer Science & Engineering
Narnarayan Shastri Institute of Technology, Jetalpur, Gujarat, India

Abstract

To address the problem of jamming under an internal threat model and consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer within the network protocol stack. The adversary or jammer exploits his internal information for launching selective jamming attacks in which specific messages of high importance are targeted. For example, an attacker will target route-request/route-reply messages at the routing layer to stop route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. The attacker may decrypt the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary should induce an enough number of bit errors in order that the packet can't be recovered at the receiver. To show that selective jamming attacks can be launched by performing real time packet classification at the physical layer. To prevent these attacks develop a schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes.

Keywords: MAC layer, jamming or blocking, Strong Hiding Commitment Scheme

I. INTRODUCTION

Wireless networks are vulnerable to various security threats due to the open nature of the wireless medium. Anyone with a transceiver will pay attention to in progress transmissions, inject spurious messages, or block the transmission of authenticate ones [1] [33]. One of the ways for degrading the network performance is by jamming wireless transmissions, in the simplest type of jamming; the adversary corrupts transmitted messages by causing electromagnetic interference within the network's operational frequencies, and in proximity to the targeted receivers [6].

The Wireless network has open nature makes it at risk of intentional interference attacks, ordinarily spoken as jamming or blocking, This jamming with wireless transmissions are often used as a launch pad for mounting Denial-of-Service attacks on wireless networks [13]. Typically, the jamming has been addressed in external threat model in which jammer is not part of network. Under this model jamming strategies include continuous or random transmission of high-power interference signal [1]. The adversaries with knowledge of internal data of protocol specifications and network secrets will launch low-effort jamming attacks that are hard to observe and counter considered as in internal threat model. In this paper, we've got addressed the matter of jamming attacks in wireless networks in internal threat model. In these attacks, jammer is active just for a few amount of time, typically it target messages of high importance. We tend to elaborate the benefits of jamming in terms of network performance degradation and jammer's effort [8]. To beat these attacks, we tend to develop a technique that stops real time packet classification by combining cryptographic primitives with physical-layer attributes.

In this paper, consider a sophisticated adversary model in which the adversary is alert to the implementation details of the network protocols. By exploiting this information, the adversary launches selective jamming attacks within which it targets specific packets of "high" importance. For instance, jamming of TCP acknowledgments (ACKs) will severely degrade the throughput of TCP connections [4]. In selective jamming the adversary is active for a short amount of time, thus spending less energy than continuous jamming. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the transmission has been completed [3] [19].

II. RELATED WORK

A. Jammers Classification

There are many various attack methods that an adversary will perform so as to interfere with different wireless nodes. The foremost accepted classification by the analysis community is: constant jammers, deceptive jammers, random jammers and reactive jammers.

1) Constant Jammers

A constant jammer incessantly emits a radio radiation that represents random bits; the signal generator doesn't follow any MAC protocol. Sender continuously senses the medium as busy. It always drops the throughput to zero for an extended amount of time till it runs out of energy.

2) Deceptive Jammers

Different from the continuous jammers, deceptive jammers don't transmit random bits instead they transmit semi-valid packets. This implies that the packet header is valid however the payload is useless. Therefore, once the legitimate nodes sense the channel they sense that there's valid traffic presently being transmitted.

3) Random Jammers

The two previous types of jammers are extremely efficient in terms of denying service. They drop the throughput to zero, however they're not energy efficient. Random jammers on the opposite hand energy efficient however a bit less efficient in denying service. They alternate between two modes. Within the initial mode the jammer jams for a random amount of time (it will behave either sort of a constant jammer or a deceptive jammer), and within the second mode (the sleeping mode) the jammer turns its transmitters off for an additional random amount of time. The energy potency is set because the magnitude relation of the length of the jamming period over the length of the sleeping amount.

4) Reactive Jammers

Another type is that the three previous varieties of jammers don't take the traffic patterns into thought that means that typically they waste energy if they're jamming once there's no traffic being exchanged within the network (active jamming). A reactive jammer tries to not waste resources by solely jamming once it senses that someone is transmittal.

B. Strong Hiding Commitment Scheme

To achieve the strong concealment property, a sub-layer referred to as the “hiding sub-layer” is inserted between the MAC and Physical layers, this sub-layer is responsible for formatting m before it's processed by the PHY layer [1]. Consider a frame m at the MAC layer delivered to the concealing sub-layer. Frame m consists of a MAC header and the payload, followed by the trailer containing the CRC code. Initially, m is permuted by applying a publicly known Permutation $\pi 1$ the aim of $\pi 1$ is to disarrange the input to the coding algorithmic program and delay the reception of essential packet identifiers like headers. In the next step, a padding function pad() appends Pad(C) bits to C, making it a multiple of the symbol size. Finally, C ‖pad(C)‖ k is permuted by applying a publicly known permutation2 [1].

When multi-hope communication is applied and packet is broadcast then each intermediate node or intermediate server has to decrypt packet and then apply inverse permutiation2 and inverse permutiation1 to check destination node for further forward packet. That is main drawback of existing system.

III. PROPOSED WORK

A Solution to the Selective jamming attack in wireless network would be the encryption of packet that is going to send. First symmetric encryption is applied to the packet data except destination. That means we hide data from adversary. After encryption of data de-commitment value that means key is send along the message by applying padding function. Now this all encrypted message C then padded bits and k all are going to be permuted. Now MAC header and this permuted data can be again encrypted by using pre-shared key. By using this method when multi-hope communication is applied then intermediate node only required one symmetric decryption to get destination address and pass it too further. Here there is no need to apply permutation to get destination node address.

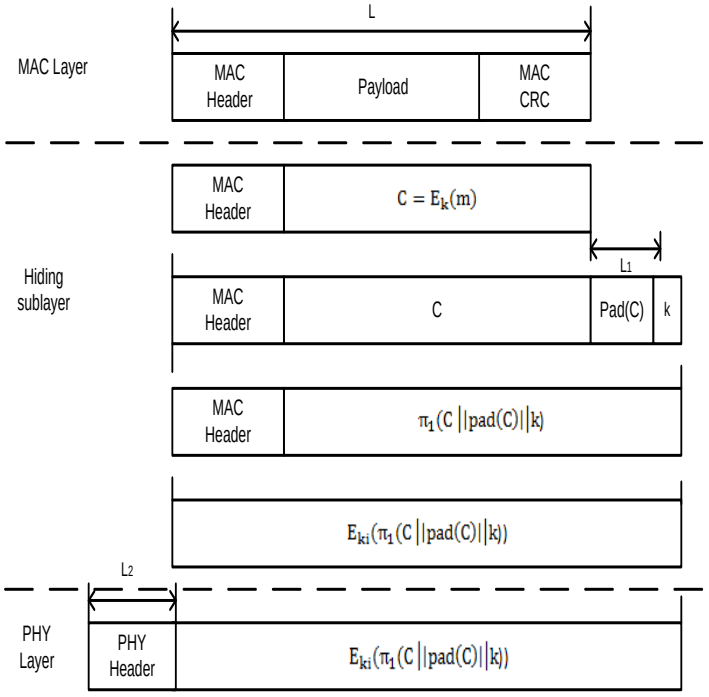

Fig. 1: Processing at MAC layer

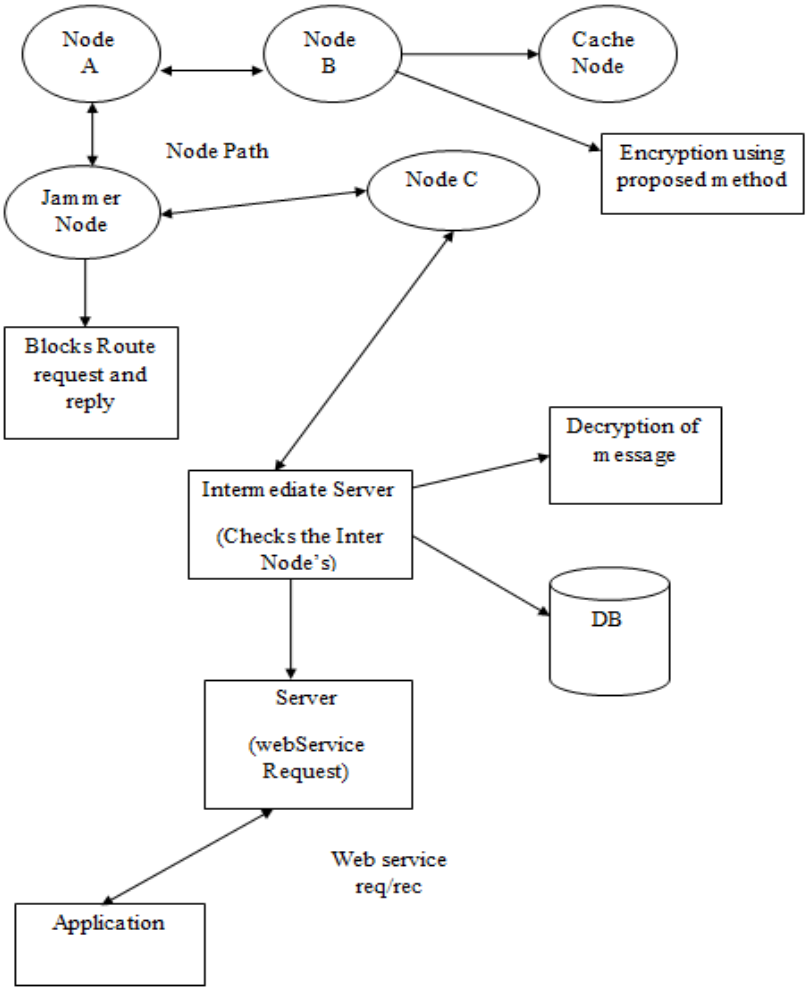

Fig. 2: Architecture Diagram of Proposed System

A. Advantages of Proposed System

- Relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes.
- Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer.
- Achieve strong security properties.

IV. SIMULATION RESULTS

Table 1:
Simulation Parameter Setup

Simulator	*NS 2.32*
Channel Type	*Wireless Channel*
Radio Propagation Model	*Two Ray Ground*
Network Interface Type	*WirelessPhy*
MAC Type	*MAC 802_11*
Interface Queue Type	*Drop tail/PriQueue*
Antenna Model	*Omni Antenna*
Queue Length	*50*
Number of Mobile Nodes	*55*
Routing Protocol	*AODV*
Traffic	*CBR*
X Dimension of Topography	*1000*
Y Dimension of Topography	*1000*
Time of Simulation End	*40s*

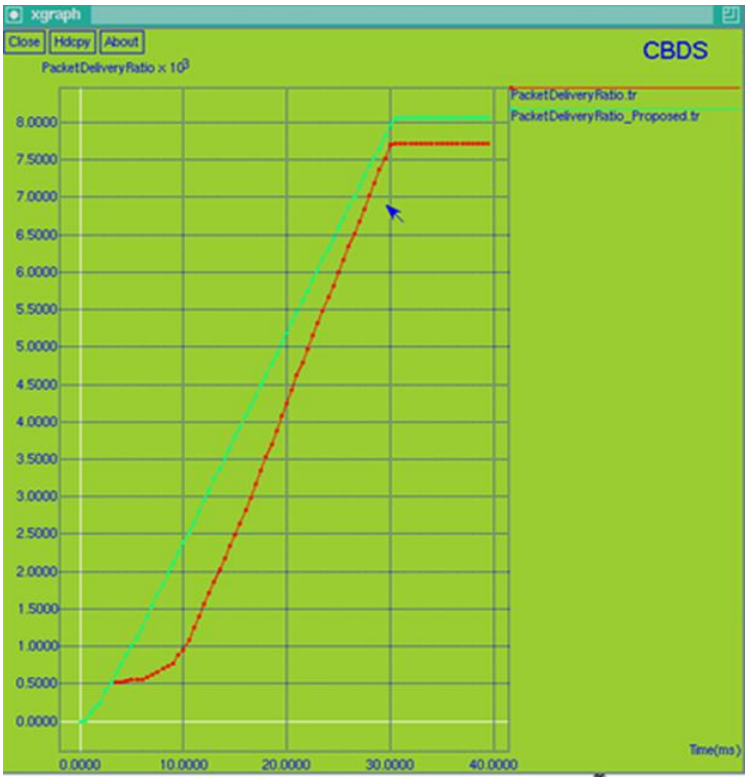

Fig. 3: Packet Delivery Ratio

Packet delivery ratio means the ratio of the number of delivered data packet to the destination. This illustrates the level of delivered data to the destination.

PDR= Number of packet receive / Number of packet send

That indicate higher value of PDR provide better performance. We can see from figure 3 till 20s PDR is 50% higher than existing system. As time increase the difference level of PDR between existing and proposed system is less. But we can see still proposed method provide better PDR and hence provide better performance of the system.

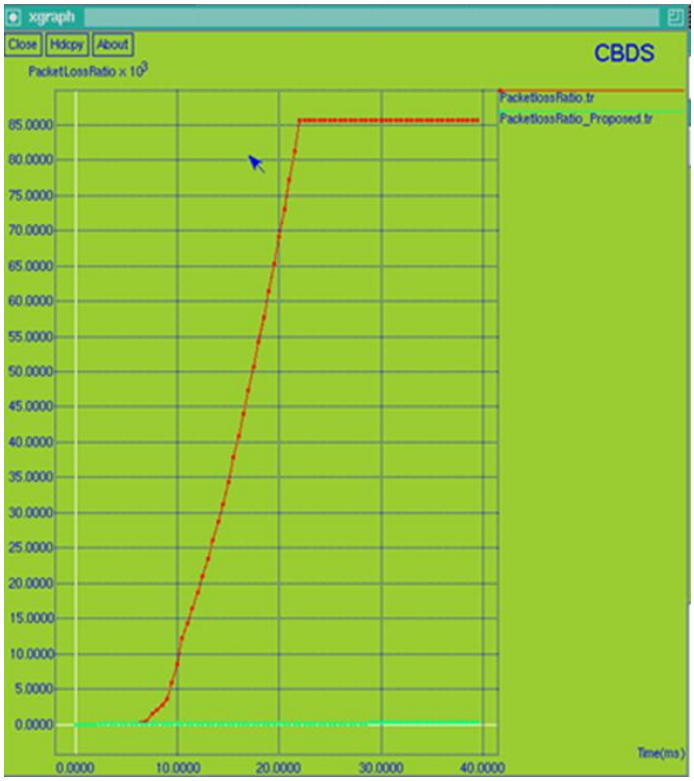

Fig. 4: Packet Loss Ratio

Packet Loss means the total number of packets dropped during the simulation. The lower value of packet loss/dropped means better performance of system.

Packet loss = Number of packet send – Number of packet received

As we provide better security against selective jamming attack in our proposed method. We use packet hiding method for preventing selective jamming attack. From figure 4 we can see packet lost ratio of our proposed system is about to zero. Hence we prevent selective jamming attack by reducing packet dropping then existing one.

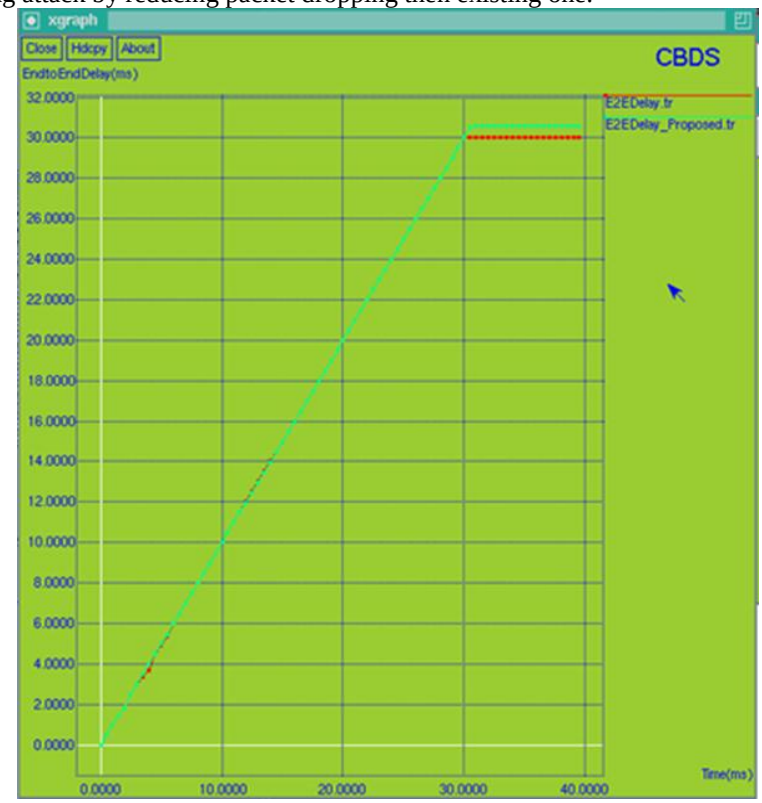

Fig. 5: E2E Delay

End-to-end Delay means the average time taken by a data packet to arrive in the destination. It also includes the delay caused by route discovery process and the queue in data packet transmission. Only the data packets that successfully delivered to destinations that counted.

End-to-end Delay= (arrive time – send time) / Number of connections

The lower value of end to end delay means the better performance of the system. We can see from figure 5 it's almost near about result of E2E of existing system.

V. CONCLUSION

In our proposed system we have proved that the open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. And also this intentional interference with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. We addressed the problem of selective jamming in wireless networks. We illustrated the effectiveness of selective jamming attacks by implementing such attacks against the TCP protocol. We showed that an adversary can exploit its knowledge of the protocol implementation to increase the impact of his attack at a significantly lower energy cost. We illustrated the feasibility of selective jamming attacks by performing real time packet classification. To prevent selective jamming, we proposed method that combines cryptographic primitives such as strong hiding commitment schemes and MD5 algorithm with physical layer attributes.

REFERENCES

[1] Packet-Hiding Methods for Preventing Selective Jamming Attacks. Alejandro Proano, Loukas Lazos. JANUARY/FEBRUARY 2012. 1, JANUARY/FEBRUARY 2012, IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, Vol. 9, pp. 101-114.
[2] Packet-Hiding Methods for Selective Jamming Attack.Ashish Kumar, Sachin Kumar Gupta, Shubham Singh. January-2013. 1, January-2013, International Journal Of Computational Engineering Research, Vol. 3, pp. 148-153. ISSN: 2250-3005.
[3] ENHANCED TECHNIQUES FOR PREVENTING SELECTIVE JAMMING ATTACKS. Abhimanyu.V, L.M.Nithya. 2013. 2013, International Journal of Computer Science and Management Research, pp. 38-42. ISSN 2278-733X.
[4] A Survey of Jamming Attack Prevention Techniques in Wireless Networks. S.Sowmya, P.D. Sheba Kezia Malarchelvi. 2014. s.l. : IEEE, 2014. ISBN No.978-1-4799-3834-6.
[5] A Medial Node Based Privacy Approaches for Preventing Selective Jamming in Wireless Networks. BKSP. Kumar Raju, R.Rajeswara Rao. 2013. 2013, IEEE.
[6] Selective Jamming Attacks in Wireless Networks. Alejandro Proano, Loukas Lazos. 2010. s.l. : IEEE ICC, 2010.
[7] An Improved Detection Method for Different Types of Jamming Attacks in Wireless Networks. Bo Yu, Lu-Yong Zhang. 2014. s.l. : IEEE 2nd International Conference on Systems and Informatics, 2014, pp. 553-558.
[8] Packet Hiding Methods for Preventing Selective Jamming Attacks.V.REDYA JADAV, T.Rohini. June-2013. 2, June-2013, International Journal of Computer Science and Electronics Engineering, Vol. 3. ISSN.0975-5664.
[9] A New Approach to Detect Radio Jamming Attacks in Wireless Networks. Ming Yu, Mengchu Zhou, Wei Su and John Kosinski. 2010. s.l. : IEEE, 2010.
[10] Puzzle Based Packet Encoding Technique for Preventing Jamming Attacks in Wireless Network. Jorvekar Priti Prakash, Gunjal Baisa L, Manish Gangwane. July-2013. 7, July-2013, International Journal of Emerging Technology and Advanced Engineering, Vol. 3, pp. 465-468. ISSN 2250-2459.
[11] A Novel Method for Preventing Selective Jamming Attacks in Wireless Networks. Ashrafunnisa, G. Sridevi. Sep - Oct. 2013. 5, Sep - Oct. 2013, International Journal of Modern Engineering Research, Vol. 3, pp. 2827-2830. ISSN: 2249-6645.
[12] ADVANCED TECHNIQUES FOR PREVENTING SELECTIVE JAMMINGATTACKS. Abhimanyu.V, L.M.Nithya.http://www.ijser.org/researchpaper%5CADVANCED-TECHNIQUES-FOR-PREVENTING-SELECTIVE-JAMMING-ATTACKS.pdf.
[13] Secure Authentication Methods for Preventing Jamming Attacks In Wireless Networks. Y. Madhavi Latha, P. Rambabu. April 2013. 4, April 2013, International Journal Of Engineering And Computer Science, Vol. 2, pp. 962-966. ISSN: 2319-7242.
[14] Combining Cryptographic Primitives to Prevent Jamming Attacks in Wireless Networks. Ngangbam Herojit Singh, A.Kayalvizhi, M.Tech. 2013. 2013, IEEE Conference Publications .
[15] Countermeasures against Energy-Efficient Jamming on Wireless Sensor Networks. Yahya ETTOUIJRI, Yassine SALIH-ALJ. 2014. s.l. : IEEE, 2014.
[16] Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution. Ali Hamieh, Jalel Ben-Othman. 2009. 2009, IEEE ICC.
[17] Encryption Techniques in Packet Hiding Methods to Prevent Jamming Attacks in Wireless Network. Rashmi B.Dhamannavar, Dr.Rashmi M.Jogdand. 2014. s.l. : 5, 2014, International Journal of Computer Science and Information Technologies, Vol. 4. ISSN: 0975-9646.
[18] Enhanced Security of Random Seed DSSS Algorithms against Seed Jamming Attacks. Thuente, Young-Hyun Oh and David J. 2012. s.l. : IEEE, 2012.
[19] A Cryptography Based Method for Preventing Selective Jamming Attack in Wireless Network. Choubey, Ms. Sonam. May-2014. 5, May-2014, International Journal of Advanced Research in Computer Science and Software Engineering, Vol. 4, pp. 1468-1470. ISSN: 2277 128X.
[20] Hiding Methods for Preventing Jamming Attacks on Wireless Networks. Asha, J. Hirudhaya Mary. July-2014. 7, July-2014, International Journal of Scientific and Research Publications, Vol. 4. ISSN 2250-3153.
[21] Jamming Attacks Prevention in Wireless Networks Using Packet Hiding Methods. Divya. S, Manohar Gosul. 3, IOSR Journal of Computer Engineering, Vol. 5, pp. 13-20. ISSN: 2278-0661.
[22] Localizing Jammers in Wireless Networks. Hongbo Liu, Wenyuan Xu, Yingying Chen, Zhenhua Liu. 2009. s.l. : IEEE, 2009.
[23] A Combined Approach for Distinguishing Different Types of Jamming Attacks Against Wireless Networks. Wyglinski, Le Wang and Alexander M. 2011. s.l. : IEEE , 2011, pp. 809-814.
[24] MITIGATION OF JAMMING ATTACKS IN WIRELESS NETWORKS. Dorus.R, Vinoth.P. 2013. s.l. : IEEE International Conference on Emerging Trends in Computing, Communication and Nanotechnology, 2013, pp. 168-171.
[25] Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications. Zhuo Lu, Wenye Wang, Cliff Wang. Aug-2014. 8, s.l. : IEEE TRANSACTIONS ON MOBILE COMPUTING, Aug-2014, Vol. 13, pp. 1746-1759.
[26] Moving-Target Defense Mechanisms Against Source-Selective Jamming Attacks in Tactical Cognitive Radio MANETs. Aleksi Marttinen, Alexander M. Wyglinski, Riku Jantti. 2014. s.l. : IEEE Conference on Communications and Network Security, 2014, pp. 14-20.
[27] Packet Hiding Methods for Preventing Selective Jamming Attacks using Swarm Intelligence Techniques. M. Rameshkumar, Dr. S. Sakthivel. Oct-2013. 10, Oct-2013, International Journal of Emerging Technology and Advanced Engineering, Vol. 3, pp. 542-545. ISSN 2250-2459.

[28] Prevention of Selective Jamming Attack Using Cryptographic Packet Hiding Methods. S.B.Gavali, A. K. Bongale, A.B.Gavali. 2014. 3, 2014, International Journal of Computer Science and Information Technologies, Vol. 5. ISSN: 0975-9646.
[29] Prevention of Selective Jamming Attacks Using Swarm intelligence Packet-Hiding Methods. R.karpagam, P.Archana. Sept- 2013. 9, Sept- 2013, International Journal Of Engineering And Computer Science, Vol. 2, pp. 2774-2778. ISSN: 2319-7242.
[30] Providing Authentication in Wireless Network to Prevent Jamming Attacks. R.Akila, T.J. Jeyaprapha, Dr. G. Sumathi. feb-2014. 2, feb-2014, International Journal of Engineering Research and Applications, Vol. 4, pp. 36-40. ISSN : 2248-9622.
[31] Research and Realization of Media Node Method to Avoid Selective Jamming. Junwei Du, Shuai Ding, Shuai Ding, Yan Wan. 2014. s.l. : IEEE Fourth International Conference on Communication Systems and Network Technologies, 2014.
[32] SAD-SJ: a Self-Adaptive Decentralized solution against Selective Jamming attack in Wireless Sensor Networks. Marco Tiloca, Domenico De Guglielmo, Gianluca Dini and Giuseppe Anastasi. 2013. s.l. : IEEE, 2013.
[33] Secure Packet Transmission for Preventing Selective Jamming Attacks. P. Narasimha Rao, B. Siva Rama Krishna, Dr. Sai Satyanarayana Reddy. July-2014. 7, July-2014, International Journal of Computer Science and Mobile Applications, Vol. 2, pp. 6-11. ISSN: 2321-8363.
[34] SELECTIVE JAMMING ATTACK PREVENTION BASED ON PACKET HIDING METHODS AND WORMHOLES. Divya Ann Luke, Dr. Jayasudha. J .S. May 2014. 3, May 2014, International Journal of Network Security & Its Applications, Vol. 6, pp. 99-105.
[35] Statistics-based Jamming Detection Algorithm for Jamming Attacks Against Tactical MANETs. Aleksi Marttinen, Alexander M. Wyglinski, Riku jantti. 2014. s.l. : IEEE Military Communications Conference, 2014, pp. 501-506.