International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802318

Jamming Attack Prevention in Wireless Network using Packet Hiding Methods

Mr.K.Navaneedhan, M.N.Dharanidharan, G.Kamalesh, K.Mohanapriyan

Muthayammal Engineering College, Rasipuram, Tamil Nadu, India

Department of Electronics and Communication Engineering, Muthayammal College of Engineering, Rasipuram, Tamil Nadu, India

Publication History: Received: 25.02.2026; Revised: 20.03.2026; Accepted: 25.03. 2026; Published: 28.03.2026.

ABSTRACT- Modern society is heavily dependent on wireless network for data Transmission. While data transmission in wireless medium, the jamming attacks occur.That selective jamming attacks can be launched by performing real-time packet classification at the physical layer.In All-Or-Nothing Transformation methods introduce a modest communication and computation overhead.In this method Block encryption algorithm is used to hiding the massages.But this algorithm not considered the Timing limits and Parameters length.To overcome this problem the Smart code generator algorithm is used.This techniques provide the strong security level in wireless Medium.

KEYWORDS: Selective jamming ,Packetclassification,Wirelessnetworks,Denial-of-Service.

I. INTRODUCTION

The wireless network is the network.It is the open nature of the medium .Anyone access in the wireless medium.so easily attacker hacking the data in wireless medium .While prevent the data ,using the cryptographic methods,jamming attacks are harder to counter. The selective jamming attacks is occur by performing real time packet classification at the physical layer. The jamming attack has considered the external threat model.These attacks develop a schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes.

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 in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of high importance are targeted. For example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow.

The jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver.

The feasibility of real-timepacket classification for launching selective jamming
attacks, under an internal threat model.The show thatsuch attacks are relatively easy to actualize by exploitingknowledge of network protocols and cryptographic primitivesextracted from compromised nodes.Develop three schemes thatprevent classification of transmitted packets in real time. The schemes rely on the joint consideration of cryptographicmechanisms with PHY-layer attributes. That analyze the security of schemes and show that they achievestrong security properties, with minimal impact on thenetwork performance.

II. LITERATURE REVIEW

2.1 Jamming and sensing of encrypted wireless ad hoc network:

In this problem consist of attacker an encrypted victim wireless ad hoc network through jamming. Jamming occur at the Transport/Network layer.sense victim packet types identify the entire header and contents of the packet ,so the packet size, timing, and sequence is available to the attacker for sensing.This paper detect only the peer nodes attacks.The encrypted victim networks in the entire packet including headers and payload are encrypted and the attacker cannot directly manipulate any of the victim communication[1].

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802318

2.2 Wormhole-based anti-jamming techniques in sensor network:

wireless sensor networks is the categoryof wireless networks to "radio channel jamming"-based Denial-of-Service (DoS) attacks.In sensed by oneor several nodes (and the sensor network is otherwise fully connected), this network cannot be operator informed on time.so sensor nodes having alarm can be transmitted to the network operator[2].

The proposed three solutions: wired pairsof sensors, relies on frequency hopping, novel conceptcalled uncoordinated channel hopping.In this approach, the nodes form low-bandwidth anti-jamming communication channelsby randomly hopping between the given set of orthogonal channels, this solution doesnot require the nodes to be synchronized.This paper not considered the synchronized nodes.

2.3 All-or-nothing encryption:

Rivest is introduced All-Or-Nothing.The brute-force search has been introduced by encryptionmode in order to solve the difficulties, while sending the pre-processing a message before encrypting it. This method having block-cipher encryption, using fixedlength blocks.

The proposeuse of a quasigroup.The main idea is to preserve a small-length key (e.g. 64-bit) for the main encryptionthat can be handled by special hardware with not enough processing power or memory.This gives the method a strong advantage, since In this paper strong encryption for devices that have minimum performance.[4]

III. EXISTING SYSTEM

3.1 Normal mode:

The normal model is used to transfer the data into the wirelessmedium.While sending the data into the wireless medium due to non security the jammer will be easilyattacks,so there is no security level in normal mode.To rectify this problem the Packet Hiding Method is established.

3.2 Hiding Based on All-Or-Nothing Transformations:

The hiding based on ANOT has been introduced by Rivest .And He has been proposed the Block encryption algorithm .By using this algorithm the receiver can receives the original data from the plaintext for detecting the Brute force attack .Due to number of ciphertext blocks there is size of changes in secret key ,so the brute force attack are slow down. So the definition has been extanded for several ANOT scheme.In this model there may be absence of at least one pseudo code-messages in all plaintext. so security level is less in this methods.

3.4 A Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Assume that the sender has a packet for Receiver. First, S constructs commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is a randomly selected key of some desired key length s (the length of k is a security parameter). Upon reception of d, any receiver R computes. Easily attacker hacking the secret key in this methods,and security level is low .

IV. PROPOSED SYSTEM

In previous technique they used the methods like secret key, puzzle setting,encrypted methods for the data hiding.An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. Moreover, even if the encryption key of a hiding scheme There to remain secret, the static portions of a transmitted packet could potentially lead to packet classification.

The proposed system using for Smart Code Generator algorithm.This algorithm used for generating the current time of the system automatically for sending the message to the authorized smart phone,then the authorized person answer for the smart code.After answering the smart code the authoried person ones can open the puzzle and answer it,then the files has been automatically receives.

International Journal of Engineering & Extended Technologies Research (IJEETR)

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802318

4.1 BLOCK DIAGRAM:

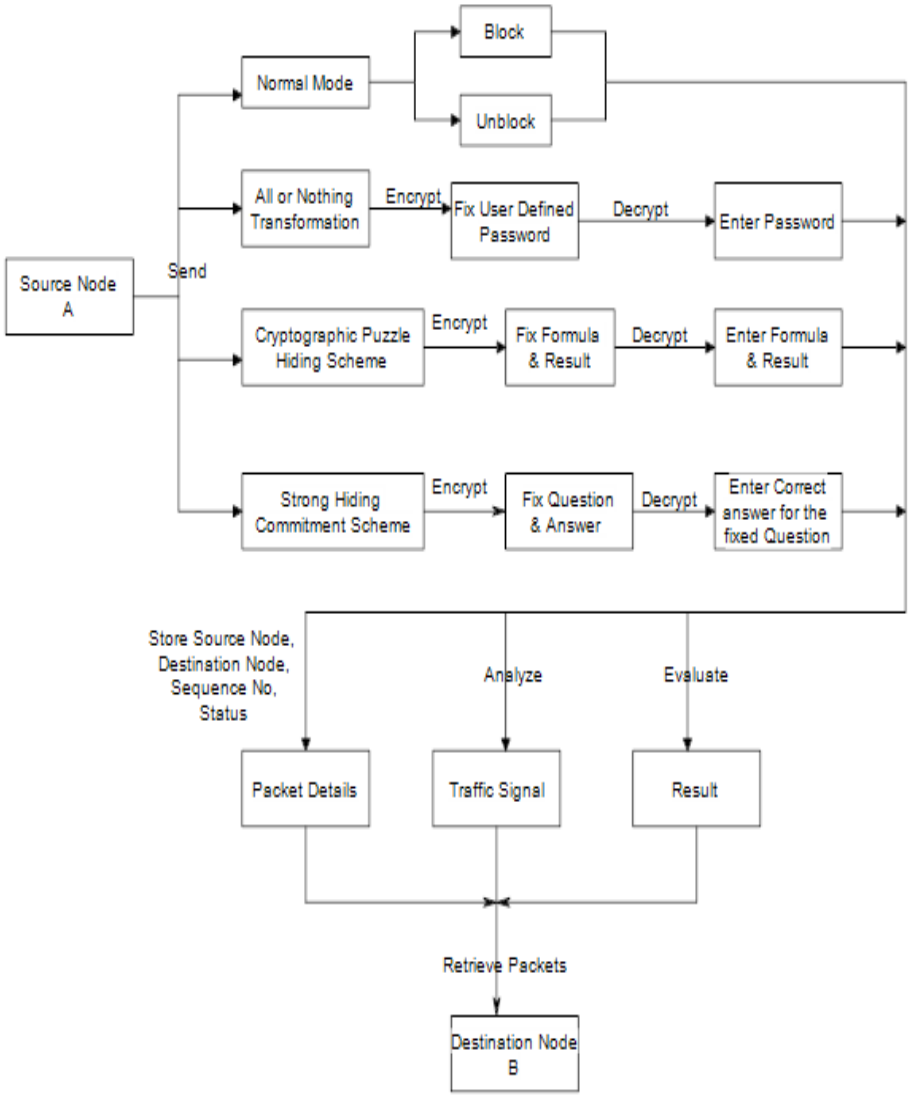

Figure No.4.1 (Block diagram of packet hiding methods)

V. SMART CODE GENERATOR: ALGORITHM

STEP 1 :Create a database and create a table named as “autocode(user-defined).

STEP 2 : In that table, Create two fields named as “auto_code” and “auto_value”.

STEP 3 :Generate Auto code Value Ranges from [0 to 9]and for each auto code value corresponding special characters willbe fixed [`~!@#$%^&*()_]

STEP 4 :Initialize Integer s1,s2,s3,i1,i2,i3,i4,i5,i6 as Integer.

STEP 5 :Assign Current system seconds to s1 which holds two digit integercharacter Where i1 = s1/10 and i2 = s1 Mod 10.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802318

STEP 6 : Assign Current system Minute to s2 which holds two digit integer character where i3 = s2/10 and i4 = s2 Mod 10.

STEP 7 :Assign Current system milliseconds to s3 which holds two digit integer character where i5 = s3/10 and i6 = s3 Mod 10.

STEP 8 :Concatenate Hash value of i1, i2,i3,i4,i5,i6 and send this secret code to recipient.

ADVANTAGES OF PROPOSED APPROACH:

- The proposed system is using for smart code algorithm.Relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes
- Findings indicate that selective jamming attacks lead to a DoS with very low effort on behalf of the jammer.
- Achieve strong security properties.
- Setting time limits.
- Limited parameters using for secret keys.

VI. CONCLUSION AND FUTURE WORK

An previous model isdeveloped three schemes that transform a selective jammer to a random one by preventing real-time packet classification.This schemes methods is having the less security level.This paper presents the Smart code generator algorithm based methods of preventing jamming attacks. This methods automatically generate the smart code.The proposed system provide for the strong security level and setting the timing limits.Our future work is to the improve the secure secret level .

REFERENCES

1. T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing ofencrypted wireless ad hoc networks. In *Proceedings of MobiHoc*, pages120–130, 2006.
2. M. Cagalj, S. Capkun, and J.-P.Hubaux.Wormhole-based anti-jammingtechniques in sensor networks.*IEEE Transactions on MobileComputing*, 6(1):100–114, 2007.
3. Y. Desmedt. Broadcast anti-jamming systems. *Computer Networks*,35(2-3):223–236, February 2001.
4. R. Rivest. All-or-nothing encryption and the package transform.*Lecture Notes in Computer Science*, pages 210–218, 1997.
5. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming:Resilience and identification of traitors. In *Proceedings of ISIT*, 2007.
6. [6] K. Gaj and P. Chodowiec.FPGA and ASIC implementations of AES.
7. *Cryptographic Engineering*, pages 235–294, 2009.
8. O. Goldreich. *Foundations of cryptography: Basic applications*. CambridgeUniversity Press, 2004.
9. B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Thetherall.Improving wireless privacy with an identifier-free link layerprotocol.In *Proceedings of MobiSys*, 2008.
10. IEEE. IEEE 802.11 standard.http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.
11. Juels and J. Brainard. Client puzzles: A cryptographic countermeasureagainst connection depletion attacks. In *Proceedings of NDSS*,pages 151–165, 1999.
12. Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, andP. Havinga. Energy-efficient link-layer jamming attacks against WSNMAC protocols. *ACMTransactions on Sensors Networks*, 5(1):1–38, 2009.
13. C.Nagarajan and M.Madheswaran - 'Stability Analysis of Series Parallel Resonant Converter with Fuzzy Logic Controller Using State Space Techniques'- Taylor &Francis, Electric Power Components and Systems, Vol.39 (8), pp.780-793, May 2011. DOI: 10.1080/15325008.2010.541746
14. C.Nagarajan and M.Madheswaran - 'Experimental verification and stability state space analysis of CLL-T Series Parallel Resonant Converter' - Journal of Electrical Engineering, Vol.63 (6), pp.365-372, Dec.2012. DOI: 10.2478/v10187-012-0054-2
15. C.Nagarajan and M.Madheswaran - 'Performance Analysis of LCL-T Resonant Converter with Fuzzy/PID Using State Space Analysis'- Springer, Electrical Engineering, Vol.93 (3), pp.167-178, September 2011. DOI 10.1007/s00202-011-0203-9
16. S.Tamilselvi, R.Prakash, C.Nagarajan,"Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller" Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802318

17. S.Tamilselvi, R.Prakash, C.Nagarajan,“ Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance” Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
18. S.Thirunavukkarasu, C. Nagarajan, 2024, “Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
19. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- ‘Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model’- *Acta Electrotechnica et Informatica Journal* , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
20. C.Nagarajan and M.Madheswaran - ‘DSP Based Fuzzy Controller for Series Parallel Resonant converter’- *Springer, Frontiers of Electrical and Electronic Engineering*, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
21. C.Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- *Iranian Journal of Electrical & Electronic Engineering*, Vol.8 (3), pp.259-267, September 2012.
22. C.Nagarajan and M.Madheswaran, “Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation” has been presented in ICTES’08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
23. Suganthi Mullainathan, Ramesh Natarajan, “An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques”, Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
24. M Suganthi, N Ramesh, “Treatment of water using natural zeolite as membrane filter”, Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
25. L. Lazos, S. Liu, and M. Krunz.Mitigating control-channel jammingattacks in multi-channel ad hoc networks. In *Proceedings of the 2nd ACM conference on wireless network security*, pages 169–180, 2009.
26. G. Lin and G. Noubir. On link layer denial of service in data wirelessLANs. *Wireless Communications and Mobile Computing*, 5(3):273–284,May 2004.
27. X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammersusing multi-layer agility. In *Proceedings of INFOCOM*, pages 2536–2540, 2007.
28. Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS:Jamming-resistant wireless broadcast communication. In *Proceedingsof INFOCOM*, San Diego, 2010.
29. R. C. Merkle. Secure communications over insecure channels. *Com-munications of the ACM*, 21(4):294–299, 1978.
30. G. Noubir and G. Lin. Low-poTherDoS attacks in data wireless lansand countermeasures. *Mobile Computing and Communications Review*,7(3):29–30, 2003.
31. OPNET. OPNETtmmodeler 14.5. http://www.opnet.com/.
32. C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc ondemanddistance vector (AODV) routing. *Internet RFCs*, 2003.
33. S.Tamilselvi, R.Prakash, C.Nagarajan,“Solar System Integrated Smart Grid Utilizing Hybrid Coot-Genetic Algorithm Optimized ANN Controller” Iranian Journal Of Science And Technology-Transactions Of Electrical Engineering, DOI10.1007/s40998-025-00917-z,2025
34. S.Tamilselvi, R.Prakash, C.Nagarajan,“ Adaptive sliding mode control of multilevel grid-connected inverters using reinforcement learning for enhanced LVRT performance” Electric Power Systems Research 253 (2026) 112428, doi.org/10.1016/j.epsr.2025.112428
35. S.Thirunavukkarasu, C. Nagarajan, 2024, “Performance Investigation on OCF and SCF study in BLDC machine using FTANN Controller," Journal of Electrical Engineering And Technology, Volume 20, pages 2675–2688, (2025), doi.org/10.1007/s42835-024-02126-w
36. C. Nagarajan, M.Madheswaran and D.Ramasubramanian- ‘Development of DSP based Robust Control Method for General Resonant Converter Topologies using Transfer Function Model’- Acta Electrotechnica et Informatica Journal , Vol.13 (2), pp.18-31,April-June.2013, DOI: 10.2478/aeei-2013-0025.
37. C.Nagarajan and M.Madheswaran - ‘DSP Based Fuzzy Controller for Series Parallel Resonant converter’- Springer, Frontiers of Electrical and Electronic Engineering, Vol. 7(4), pp. 438-446, Dec.12. DOI 10.1007/s11460-012-0212-0.
38. C.Nagarajan and M.Madheswaran - ‘Experimental Study and steady state stability analysis of CLL-T Series Parallel Resonant Converter with Fuzzy controller using State Space Analysis’- Iranian Journal of Electrical & Electronic Engineering, Vol.8 (3), pp.259-267, September 2012.

|ISSN: 2322-0163| www.ijeetr.com | A Bimonthly, Peer Reviewed, Scholarly Indexed Journal |

| Volume 8, Issue 2, March - April 2026 |

DOI:10.15662/IJEETR.2026.0802318

39. C.Nagarajan and M.Madheswaran, “Analysis and Simulation of LCL Series Resonant Full Bridge Converter Using PWM Technique with Load Independent Operation” has been presented in ICTES’08, a IEEE / IET International Conference organized by M.G.R.University, Chennai.Vol.no.1, pp.190-195, Dec.2007
40. Suganthi Mullainathan, Ramesh Natarajan, “An SPSS and CNN modelling based quality assessment using ceramic materials and membrane filtration techniques”, Revista Materia (Rio J.) Vol. 30, 2025, DOI: https://doi.org/10.1590/1517-7076-RMAT-2024-0721
41. M Suganthi, N Ramesh, “Treatment of water using natural zeolite as membrane filter”, Journal of Environmental Protection and Ecology, Volume 23, Issue 2, pp: 520-530,2022
42. Yoong Choon Chang, Sze Wei Lee and Ryoichi Komiya, Members, IEEE “A Low-Complexity Unequal Error Protection of H.264/AVC Video Using Adaptive Hierarchical QAM” IEEE Transactions on Consumer Electronics, Vol. 52, No. 4, NOVEMBER 2006.
43. Y. Pei and J.W. Modestino “Cross-Layer Design for Video Transmission over Wireless Rician Slow-Fading Channels Using an Adaptive Multiresolution Modulation and Coding Scheme” Hindawi Publishing Corporation EURASIP Journal on Advances in Signal Processing Volume 2007, Article ID 86915, 12 pages doi:10.1155/2007/86915.