ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

Reducing Jamming Attacks Using Packet Hiding Methods in Network

Kakarapalli Satya
M.Tech Student,
Dept of CSE,
BVC Engineering College,
Odalarevu.

Asapu Satya Mallesh
Assistant Professor,
Dept. of CSE,
BVC Engineering College,
Odalarevu.

Abstract:

In the network environment most of the time there could be more chances of the attacks. That means most of the time does not guarantee about the packets can be easily transfer over the network.It affects the network performance degrade.To overcomove problem of network traffic and performance in this paper we address the wireless networks are more sensitive to the Denial-of-Service (DoS) attacks. The existing system is based on Spread Spectrum (SS). This technique mainly focuses on an external threat model. Jamming has been addressed under an external threat model In wireless network the communications between nodes take place through broadcast communication. That is why, if an attacker present within the network can easily eavesdrop the message sent by any node. The main attack present in the wireless network is the selective jamming attack. This type of attack mainly focuses a single node termed as target node.

Attacker always tries to block the message sent by the target node. This leads to the Denial-of-Service attack. We are proposing a new method to prevent the selective jamming attack in an internal threat model. A wormhole is used, which will generate an alarm to indicate the presence of jammer and sent IP address of jammer node to all other nodes in the network. Using a method called packet hiding, we can send message through the network even though a jammer is present. This method is based on the technique called Strong Hiding Commitment Scheme (SHCS). Here, the access point in a network region becomes the wormhole whenever it finds out any node that violates the rules in a particular network region. That node is then considered as a jammer node.

The wormhole sends IP address of jammer to all other nodes. Wormhole then prevents the jamming activity of the jammer by encrypting the source ID of message along with the message packet.So that the jammer is unable to identify its target node and the source can forward its message safely through jammer node itself.

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

AIM:

To show that selective jamming attacks can be launched by performing real time packet classification at the physical layer. To mitigate these attacks develop a schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes.

SYNOPSIS:

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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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.

Eavesdropper jammer:

Listens and records wireless traffic in channel(s).To defend the above from jammers, the first step is to detect the existence of jammer because many other factors can also result in the similar appearance like jammer performed such as low SNR (Signal Noise Ratio), battery running out of power or receiver moving out of the range. A lot of detection methods have been proposed such as Signal Strength detection, Carrier sensing time detection and PDR (Packets Delivery Ratio) detection, however each of which has their own weak point. The current state of art is Signal Strength Consistency Checks which can differentiate jamming from normal signals. However, the only problem of Strength Consistency Checks is it cannot differentiate between the various categories of jamming attacks. To enable the network to perform defense strategies more effectively such as saving power or quickly enough reaction, distinguishing the type of different jamming attacks is necessary.

1. INTRODUCTION:

The wireless networks are more sensitive to the Denial-of-Service (DoS) attacks [1]. In almost every case, jamming causes a denial of service type attack to either sender or receiver. The easiest form of jamming a wireless network communication is to continually transmit useless data to the node where the server becomes overloaded. Most people have no idea if a jamming signal is in use. It appears as if there is no service. This attack makes the network resource unavailable to its legitimate users. The existing system is based on Spread Spectrum (SS). This technique mainly focused on an external threat model. In broadcast communication, if an attacker present within the network can easily drop the message sent by any node. In selective jamming attack, the attacker always tries to block the message sent by its target node and it leads to the Denial-of-Service attack [1] [2].

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. 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 [12], [17], [36], [37]. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal [25], or several short jamming pulses [17].

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 [25], [36]. However, adopting an "always-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect [17], [36], [37]. Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications [25], or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats [37]). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties.

These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise, neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information. In this paper, we address the problem of jamming under an internal threat model. We 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.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

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. To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission.

Such strategy can be actualized either by classifying transmitted packets using protocol semantics [1], [33], or by decoding packets on the fly [34]. In the latter method, 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 [34]. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

In 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. 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.

This strategy has several disadvantages.

- First, the adversary has to expend a significant amount of energy to jam frequency bands of interest.

- Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect.

Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model.

DISADVANTAGES :

- Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions.

- The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming.

- Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones.

- Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

In current System, we address the problem of jamming under an internal threat model. We 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.

To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly.

To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes.

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 were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

ADVANTAGES OF CURRENT 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 a DoS with very low effort on behalf of the jammer.

- Achieve strong security properties.

LITERATURE SURVEY:

Literature survey is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy n company strength. Once these things r satisfied, ten next steps is to determine which operating system and language can be used for developing the tool. Once the programmers start building the tool the programmers need lot of external support. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration r taken into account for developing the proposed system.

RELATED WORK:

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s [15].Recently, several alternative jamming strategies have been demonstrated [11], [12], [19], [20]. Xuet. al. Categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected.

Intelligent attacks which target the transmission of specific packets were presented in [8], [18]. Thus considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer. Considered (a) (b). We analyze the security of our schemes and show that they achieve strong security properties, with minimal impact on the network performance.

We investigate the feasibility of real-time packet classification for launching selective jamming attacks. We show that such attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes. Our finding indicates that selective jamming attacks lead to a DoS with very low effort on behalf of the jammer.

To mitigate such attacks, we develop schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack.

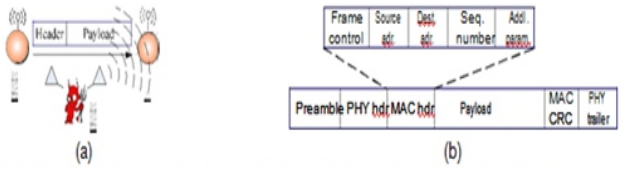


Fig. 1 (a) Realization of a selective jamming attack. (b) a generic frame format for a wireless network.

IMPLEMENTATION:

Implementation is the stage of the project when the theoretical design is turned out into a working system. Thus it can be considered to be the most critical stage in achieving a successful new system and in giving the user, confidence that the new system will work and be effective.The implementation stage involves careful planning, investigation of the existing system and it's constraints on implementation, designing of methods to achieve changeover and evaluation of changeover methods.

Network module:

We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in uni-cast mode and broadcast mode. Communications can be either unencrypted or encrypted.

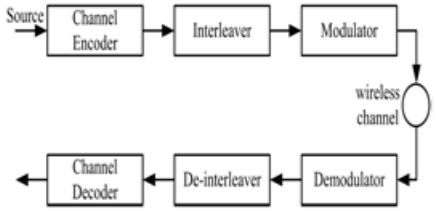
ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre-shared pair wise keys or asymmetric cryptography.

Real Time Packet Classification:

Consider the generic communication system depicted in Fig. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinter leaved, and decoded, to recover the original packet m. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification.

This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.



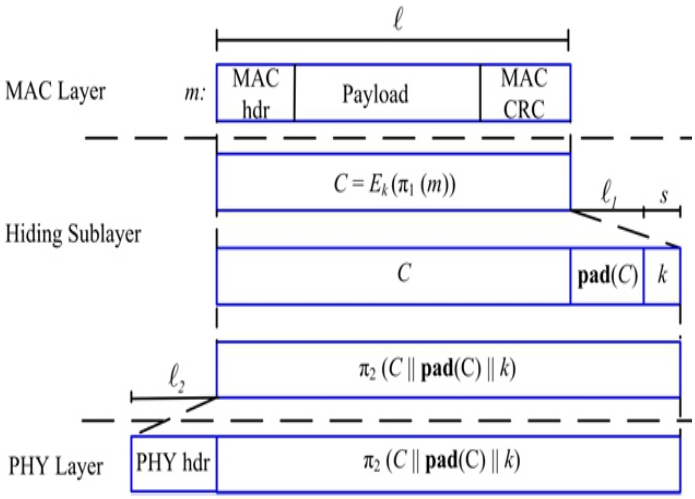
Selective Jamming Module:

We illustrate the impact of selective jamming attacks on the network performance. Implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

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. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block.

Strong Hiding Commitment Scheme (SHCS):

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.



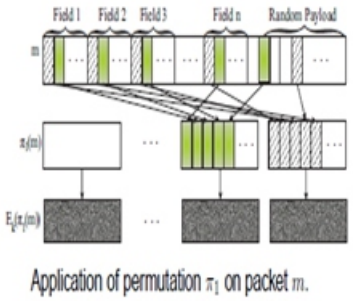
The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed . If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver.

Cryptographic Puzzle Hiding Scheme (CPHS):

we present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.



Application of permutation π_1 on packet m.

CONCLUSION:

In this way, we address the problem of selective jamming attacks in networks. We considered an internal adversary model in which the jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. We show that the jammer can classify the packets in real time by decoding the first few symbols of an ongoing transmission. We evaluate the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort. We are developing and survey on three schemes that transform a selective jammer to a random one by preventing real-time packet classification.

REFERENCES:

[1] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

[2] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormhole-based antijamming techniques in sensor networks. IEEE Transactions on Mobile Computing, 6(1):100–114, 2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.

[4] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper. Intelligent sensing and classification in ad hoc networks: a case study. Aerospace and Electronic Systems Magazine, IEEE, 24(8):23–30, August 2009.

[5] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.

[6] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.

[7] O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall. Improving wireless privacy with an identifier-free link layer protocol. In Proceedings of MobiSys, 2008.

[9] IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/ download/802.11-2007.pdf, 2007.

[10] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connectison depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.

[11] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, and P. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACM Transactions on Sensors Networks, 5(1):1–38, 2009.

[12] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.

[13] G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.

[14] X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In Proceedings of INFOCOM, pages 2536– 2540, 2007.

[15] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010.

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

[16] R. C. Merkle. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978.

[17] G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. Mobile Computing and Communications Review, 7(3):29–30, 2003.

[18] OPNET. OPNETtm modeler 14.5. http://www.opnet.com/.

[19] C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc ondemand distance vector (AODV) routing. Internet RFCs, 2003.

[20] C. P ¨opper, M. Strasser, and S. Capkun. Jamming-resistant broadcast ˇ communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[21] R. Rivest. All-or-nothing encryption and the package transform. Lecture Notes in Computer Science, pages 210–218, 1997.

[22] R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timedrelease crypto. Massachusetts Institute of Technology, 1996.

[23] B. Schneier. Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, 2007.

[24] SciEngines. Break DES in less than a single day. http://www. sciengines.com, 2010.

[25] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.

[26] D. Stinson. Something about all or nothing (transforms). Designs, Codes and Cryptography, 22(2):133–138, 2001.

[27] D. Stinson. Cryptography: theory and practice. CRC press, 2006.

[28] M. Strasser, C. P ¨opper, and S. Capkun. Efficient uncoordinated fhss ˇ anti-jamming communication. In Proceedings of MobiHoc, pages 207– 218, 2009.

[29] M. Strasser, C. P ¨opper, S. Capkun, and M. Cagalj. Jamming-resistant ˇ key establishment using uncoordinated frequency hopping. In Proceedings of IEEE Symposium on Security and Privacy, 2008.

[30] P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of PIMRC, 2007.

[31] P. Tague, M. Li, and R. Poovendran. Mitigation of control channel jamming under node capture attacks. IEEE Transactions on Mobile Computing, 8(9):1221–1234, 2009.

[32] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng. On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming. In Proceedings of WiSec, 2011.

[33] D. Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.

[34] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. Reactive jamming in wireless networks: How realistic is the threat? In Proceedings of WiSec, 2011.

[35] W. Xu, W. Trappe, and Y. Zhang. Anti-jamming timing channels for wireless networks. In Proceedings of WiSec, pages 203–213, 2008.

[36] W. Xu, W. Trappe, Y. Zhang, and T. Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In Proceedings of MobiHoc, pages 46–57, 2005.

[37] W. Xu, T. Wood, W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. In Proceedings of the 3rd ACM workshop on Wireless security, pages 80–89, 2004.

ABBREVIATIONS:

TCP/IP : Transmission Control Protocol/Internet Protocol
EIS : Enterprise Information Systems
RMI : Remote Method Invocation
BIOS : Basic Input/output System

ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

SITES REFERRED:

http://java.sun.com

http://www.sourcefordgde.com

http://www.networkcomputing.com/

http://www.roseindia.com/

http://www.java2s.com/

About Authors:

Kakarapalli Satya
presently pursuing Master of Technology on computer science and engineering from "BVC Engineering College, Odalarevu", under "JNTU Kakinada ".She completed her Master's of Science on Computer Science from "VSL College for Women's,Kakinada "Under" Andhra University Visakhapatnam". Her area of Interest is Networking.

Asapu Satya Mallesh
currently working as Assistant Professor at "BVC College of Engineering, Odalarevu", Under Computer Science and Engineering. He Completed his Master of Technology on Computer Science and Engineering at "BVC College of Engineering, Odalarevu". His area of Interest is Networking.