ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Packet Concealing From Discriminating Selective Jamming Attacks Using Prevention Methods

Mr. A.Rajesh Kumar[1], Mrs. R.Bharathi[2]

P.G Scholar, Department of CSE, M.Kumarasamy College of Engineering, Thalavapalayam, Karur, Tamilnadu, India[1]

Asst Professor, Department of CSE, M.Kumarasamy College of Engineering, Thalavapalayam, Karur, Tamilnadu, India[2]

ABSTRACT— The wireless medium leaves it vulnerable to deliberate interference attacks which is called as jamming. This deliberate interference with wireless transmissions can be used a rise for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been address under an outdoor threat model. Though, adversaries with internal knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect the jamming attack and it is unable to count. The problem of selective jamming attacks in wireless networks is addressed. The selective jamming attack is defined as the attack in which the adversary is active only for a short duration period. This type of attack is selectively targeting the messages of high importance. The advantages of selective jamming in terms of network performance demotion and adversary effort is presented in two case study methods. First a selective attack is implemented on TCP. Second the selective jamming attacks implemented on routing. The selective jamming attacks can be explained by performing real-time packet classification at the physical layer. To reduce the selective jamming attack, the four types of schemes are incorporated that can be prevent real-time packet classification by combining the cryptographic primitives with physical-layer attributes. The four types of schemes are Digital Signature Based Transformation (DSBT), All-Or-Nothing Transformations (AONT), Cryptographic Puzzle Hiding Scheme (CPHS), Strong Hiding Commitment Scheme (SHCS).The security of methods is tested and this will evaluate the computational and communication overhead.

KEYWORDS-Selective Jamming, Dos, Wireless Network, Packet Classification methods Digital Signature Based Transformation (DSBT), All-Or-Nothing Transformations (AONT), Cryptographic Puzzle Hiding Scheme (CPHS), Strong Hiding Commitment Scheme (SHCS).

I. INTRODUCTION

Wireless Local Area Networks (WLANs) are becoming an increasingly important technology that is bringing the world nearer together. WLANs are used in all over areas, such as educational area, agriculture area, pharmaceuticals, manufacturing, transportation, military, and research area. Hence, the importance of Wireless Local Area Network (WLAN) security is notable. WLANs can provide two types of popular styles. They are client-server networks and ad-hoc networks. The discrepancy between these two networks is that client-server networks routers or use access point to transmit data, but ad-hoc networks do not believed on any pre-existing transmitters. For example all the nodes in an ad-hoc network participate in the routing process by forwarding messages together. According to The Institute of Electrical and Electronics Engineers (IEEE) 802.11g standards (IEEE Org., 2012) issues some standard information about the wireless networks. All wireless network nodes transmit data packets in various channels. Since channels in WLANs are definite by frequencies, they are impressionable to nasty jamming attacks. It is easy for attackers to perform send more than of useless packets in a specific frequency. Jamming attacks attempt to provide the system crash by torrent it with unnecessary traffic, and use all the resources in the network so users in the network cannot properly connect to the system. It is consistently used by unauthorized person to break networks and system performance, because of ease rise and security issues.

II. LITERATURE SURVEY

2.1 Jamming Attacks

Jamming attack cause the collision in networks transmission medium and the attacker can perform various actions in the normal flow of data transmission that kind of node is called as jamming node. It acts as original sender behavior. So easily hacker or attacker can retrieve or modify that original transmission data. There are lot of jamming method are available in the network models. Constant jammer send jamming signal of certain duration at a constant interval. Deceptive jammers send regularly to inject packet without any gap between transmissions. Random jammer sends jamming signal of certain duration at a randomly chosen interval. It is more power efficient jamming. Reactive jammer sends signal of certain duration only when communication is present in channel sense packet transmit immediately transmission radio signal in order to cause of collision at receiver and selective jamming attacker can perform only high confidential message only.

2.2 Time-lock puzzles and timed-release Crypto

There are two natural approaches to implementing timed-release crypto. 1) Use "time-lock puzzles "computational problems that cannot be solved without running a computer continuously for at least a certain amount of time. 2) Use trusted agents who promise will not to reveal certain information until a specified date.

2.3 Control Channel Jamming: Resilience and identification of Traitors

The main objective of the control channel jamming is to avoid jamming and making the channel in flexible manner. To avoid jamming some solutions are proposed they are 1) Instead of mapping the control channels to static location, it randomly (dynamic) maps them according to a cryptographic function. 2) Mapping is unpredictable to external attackers. 3) Thus it prevents the external attacker from destroying the control channels.

2.4 Anti-jamming Timing Channels for Wireless Networks

The main objective behind the Anti-jamming Timing Channels for Wireless Networks is 1) Creation of low-bit rate connection at the top of the PHY/LINK layers. 2) Low-bit rate channel is constructed as a timing channel. 3) It restores the availability of a communication link in the presence of interference. 4) Jamming detection and mapping the jammed region is possible through use of network utility metrics.

2.5 Algorithm

1. Symmetric encryption algorithm
2. Brute force attacks against block encryption algorithms

The solution is based on All-Or-Nothing Transformations (AONT) that introduces a simple communication and computation overhead. These transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms. An AONT service as a publicly known and wholly invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm.

2.8 Algorithm Description

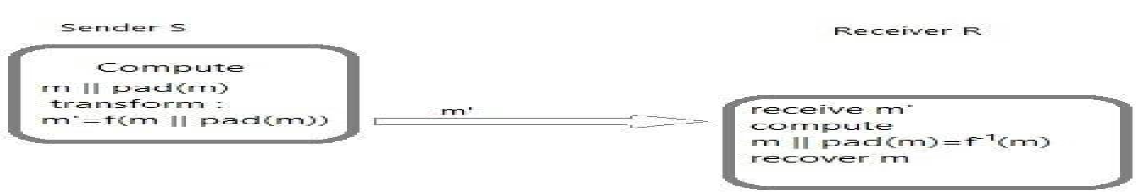

Fig A. The AONT-based Hiding Scheme (AONT-HS)

The Package Transform- In the package transforms, given a message m and a random key k′, the output pseudo-messages computed as follows:

Message 'i = message i Ek'

(i), for i=1,2,……..x, message'x+1 = k' e_1 e_2 e_3 …………. e_x ,

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

Where e_i = Ek0 (message'i □ i), for i = 1, 2. . . x, and k0 is a fixed publicly-known encryption key. With the arrive of all pseudo-messages message m is recovered as follows:

k' = message'x+1 □ e_1 □ e_2 □ e_3 □ ………….. □ e_x ,

Message i = message'i □ Ek'

(ii)for i=1, 2, 3 …………….x,

Note that if any message'i is unknown, any value of k′ is feasible, because the corresponding ei is not known. Therefore, Ek'(i) cannot be retrieved for any i, making it infeasible to obtain any of the message i.

2.8.1 Hiding Sub-layer Details

AONT-HS is implemented at the hiding sub-layer residing between the MAC and the PHY layers. In first step, m is padded by applying function pad() to adjust the frame length so that no padding is needed at PHY layer, and the length of m becomes a multiple of the length of the pseudo-messages message′i. That will ensure that all bits of the transmitted packet are part of the AONT. In the next step, m||pad(m) is distribute to x blocks, and the AONT f is applied. Message message′is delivered to the PHY layer. At the receiver, it provide the inverse transformation f−1 is applied to obtain m||pad(m). The padded bits are cancelled and the original message m is retrieve. The steps of AONT-HS are shown in Figure. A.

III. ARCHITECTURE

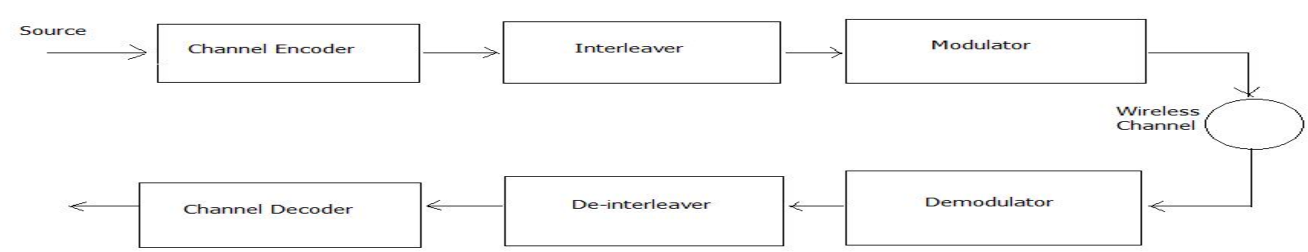

Fig 1. Generic Communication Classification Diagram

The generic communication classification diagram will show interleaved process of original message keep into adversary here source message enter into channel encoder. The channel encoder can perform interleaved process before modulator it is transmitted over the wireless channel. At another receiver end the signal is demodulator perform de-interleaved .that process used to rearrange original message again using of decoder channel.

IV. PROBLEM FORMULATION

4.1 Existing System

Jamming attacks are much difficult to counter and more security problems rise in this case. They have been shown to actualize service Denial-of-Service (DoS) attacks against wireless networks. In the simple form of jamming, the adversary interferes with the entries of messages by transmitting a continuous jamming signal, or more than short jamming pulses jamming attacks have been considered under an external threat model. In this the jammers is not part of the network. Below this model, jamming strategies include the continuous or random transmission of high-power interference signals. So interference occurs easily in transmission medium. And also an eavesdropping occurs, so easily trusted person original information leakage.

4.2 Proposed System

The problem of jamming is under an internal threat model resolved. To count a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The rival exploits the internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. Example, a jammer can target route-request/route-reply messages at the routing layer to prevent route discovery, or purpose of TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. Throw the selective jamming attacks, the rival or adversary must be capable of implementing a

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

"classify-then-jam" strategy before the completion of a wireless transmission. Similar that strategy can be actualized either by classifying transmitted packets using protocol semantics, by decoding packets on the fly.

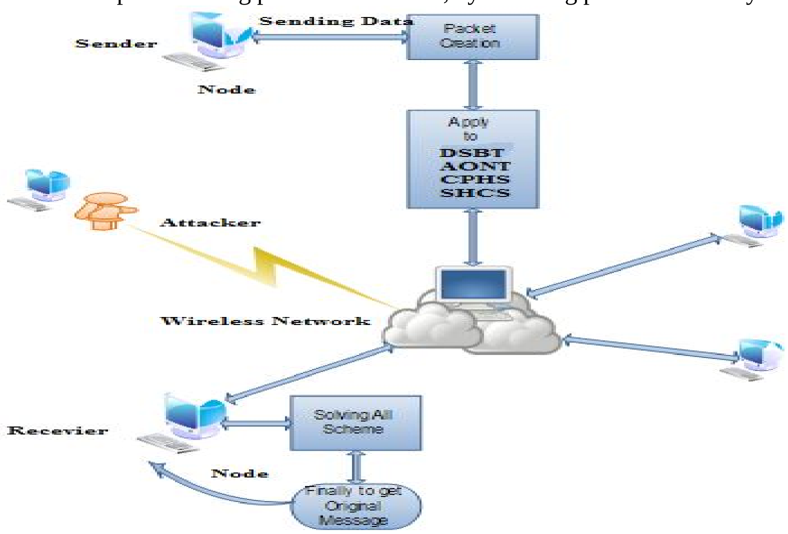

Fig 2. Architecture Diagram

In the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source address and destination address. Following classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. The Selective jamming requires intimation knowledge of the physical (PHY) layer, as well as of the specifics of upper layers. To expand four types of schemes that can be preventing real-time packet classification by combining cryptographic primitives with physical-layer attributes. The testing of the security of these methods, to evaluate, to reduce their computational and communication overhead over the transmission signals. It improves the network throughput by avoiding interference and also provide full security guarantee.

Even though there is a strong hiding scheme the trusting cannot be made on the person who is working in enterprise. Because the person who worked in enterprise and left out later may reveal confidential message about the scheme. Therefore the attacker can easily have the access over the scheme and may possibly break the security scheme. To avoid that the digital signature based Transformation is introduced. This technique will make the message more secure and make the schemes more strong from the attackers.

V. MODULES

1. Key Preprocessing and Packet Conversion
2. DSBT Technique
3. AONT Scheme
4. CPH Scheme
5. SHC Scheme
6. Packet Transmission and Recovery

VI. MODULE DESCRIPTIONS

6.1 Key preprocessing and Packet conversion

The wireless network is stated as a collection of nodes connected via wireless links. In that, the term Key Processing is defined as a process of pre- distribution of the keys. The symmetric key is provided by the server for the set of nodes. To acquire the symmetric key the node should join the network. For communicating from one node to

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

another node the symmetric key is used. But the nodes have various requirements in case of node communication directly or indirectly. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. The nodes may prefer both unicast and broadcast mode. Messages can be either decrypted or encrypted. Encrypted broadcast messages, symmetric keys are shared among all intended receivers.

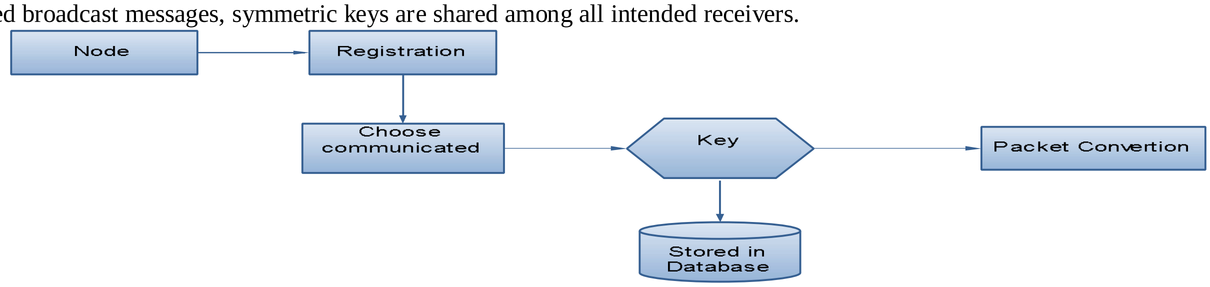

Fig 3. Key Preprocessing and Packet Conversion

Messages can be either decrypted or encrypted. Encrypted broadcast messages, symmetric keys are shared among all intended receivers. Depending on the size of the physical layer capacity the desired transmission packet is converted by the sender after choosing the destination.

6.2 Digital Signature Based Transformation (DSBT)

A digital signature is a mathematical scheme for demonstrating the authenticity of a digital document or message. A valid digital signature gives a recipient reason to believe that the message was created by a known sender, such that the sender cannot deny have to sent the message (authentication and non-repudiation) and that the message was not altered in transit (integrity). Digital signatures are commonly used for financial transactions software distribution and in other cases where it is important to detect forgery or tampering.

Digital signatures employ a type of asymmetric cryptography. For a messages sent through a non secure channel, a properly implemented digital signature gives the receiver reason to believe the message was sent by the claimed sender. Digital signatures are equivalent to traditional handwritten signatures in many respects, but a properly implemented digital signature is more difficult to forge than the handwritten type. Digital signature schemes, in the sense used here, are cryptographically based, and must be implemented properly to be effective. Digital signatures can also provide non-repudiation, meaning that the signer cannot successfully claim they did not sign a message, while also claiming their private key remains secret; further, some non-repudiation schemes offer a time stamp for the digital signature, so that even if the private key is exposed, the signature is valid. Digitally signed messages may be anything representable as a bit string e.g., contracts, electronic mail, or a message sent via some other cryptographic protocol.

Digital Signature Based Transformation (DSBT) that introduces a secure communication and more computation overhead. It consists of three generating techniques. A key generation algorithm that selects a private key uniformly at random from a set of possible private keys. The algorithm outputs the private key and a corresponding public key.

1) A signing algorithm that, given a message and a private key, produces a signature.
2) A signature verifying algorithm that, given a message, public key and a signature, either accepts or rejects the message's claim to authenticity.

Some of the properties of the digital signature which is implemented are, 1) Signature generated from a fixed message and fixed private key should verify the authenticity of that message by using the corresponding public key. 2) It should be computationally infeasible to generate a valid signature for a party without knowing that party's private key.

6.3 All-or-Nothing Transformation

All -Or- Nothing Transformations (AONT) Fig A. that introduces a simple communication and computation overhead. Like transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms. The AONT Transformation which give the identity to sender. The sender is only known by his/her Pseudonym.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

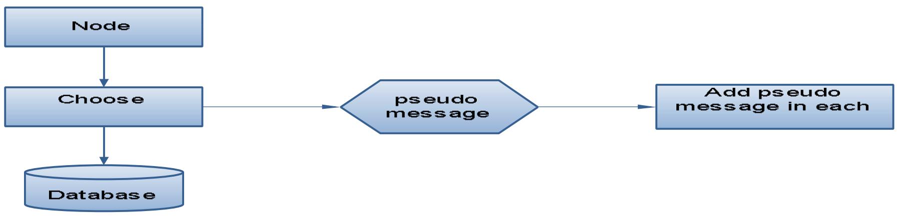

Fig 4. All-or-Nothing Transformation

The sender will send the message along with his identity which is named as the Pseudo message. In which the recipient can be authenticated only if the recipient knows only about the pseudonym of the sender. The AONT service as a publicly known and wholly invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm.

6.4 Cryptographic Puzzle Hiding Scheme (CPHS)

Cryptographic Puzzle Hiding Scheme (CPHS) is technique which is used to provide the security in non-secure channel. The time lock puzzle is constructed that is fully based on the iterative application of a precisely controlled number of modulo operations in this process. The sender will randomly generate the puzzle for each and every process and set the time for solving the puzzles. The receiver at the other end decodes the packet when all the packets are received. Since here the Selective jamming attack is taken care the time-lock puzzles used to reduce the packet accessing of time. Because the selective jammers will be stay awaken for the short period of time in the network and at other time they will stay idle.

Fig 5. Cryptographic Puzzle Hiding Scheme

The main objective 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 duration time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. Advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. Though, it has higher computation and communication overhead. Cryptographic puzzles are primitives genuine suggested by Merkle as a method for establishing a secret over an insecure channel. For preventing Dos attacks they detect a wide range of applications to provide broadcast authentication and key escrow schemes.

6.5 Strong Hiding Commitment Scheme (SCHS)

The strong hiding commitment scheme (SHCS) is based on symmetric cryptography. The 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 in which the symmetric encryption at the sender and one symmetric decryption at the receiver. Because the main header information is permuted as a trailer and encrypted, In all receivers are vicinity of a sender must receive the entire packet and decrypting it, earlier the packet type and destination can be determined. Though, in wireless protocols such as 802.11 standard, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed and some parts of the MAC header are deemed not to be useful information to the jammer, that person can remain unencrypted in the header of the packet, so avoiding the decryption operation at the receiver.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization) Vol.2, Special Issue 1, March 2014

Proceedings of International Conference On Global Innovations In Computing Technology (ICGICT'14)

Organized by

Department of CSE, JayShriram Group of Institutions, Tirupur, Tamilnadu, India on 6th & 7th March 2014

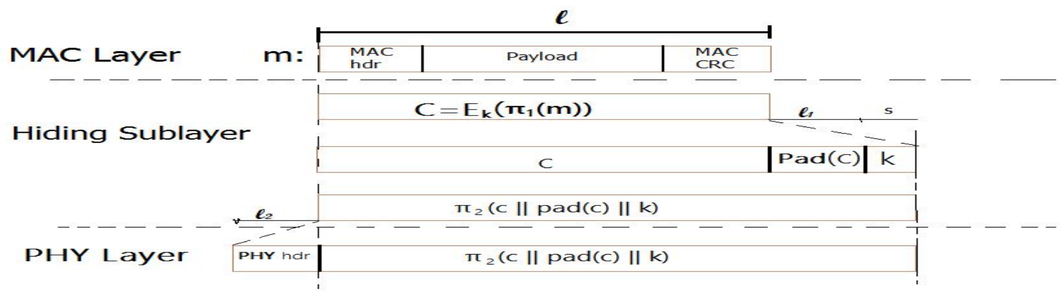

Fig 6. Layers in Networks

A strong hiding commitment scheme, which is based on symmetric cryptography. To reduce the overhead of SHCS, the decommitment value d (i.e., the decryption key k) is carried in the same packet as the committed value C. This saves the extra packet header needed for transmitting d individually. To achieve the strong hiding property, a sub layer called the "hiding sub layer" is inserted between the MAC and the PHY layers.

The sub layer is responsible for formatting m before it is processed by the PHY layer. Padding and the Permutation are the SHCS scheme which is mainly used for security. Due to implementation the each frame in this process contains the source and destination address, CRC value, MAC header details, length of the frame.

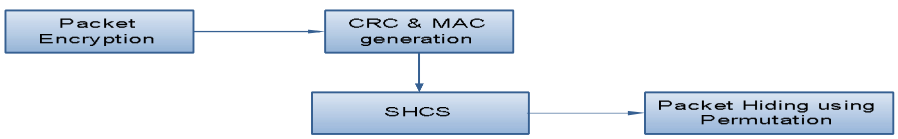

Fig 7. Strong Hiding Commitment Scheme

6.6 Packet Transmission and Recovery

The packet is send from sender to the receiver. The modulator in the system which will receive the bit stream of the packet and it modulates the packet further and it will transform those packets into suitable format for transmission. The recipient who needs to receive the packets may be within a communication range or without.

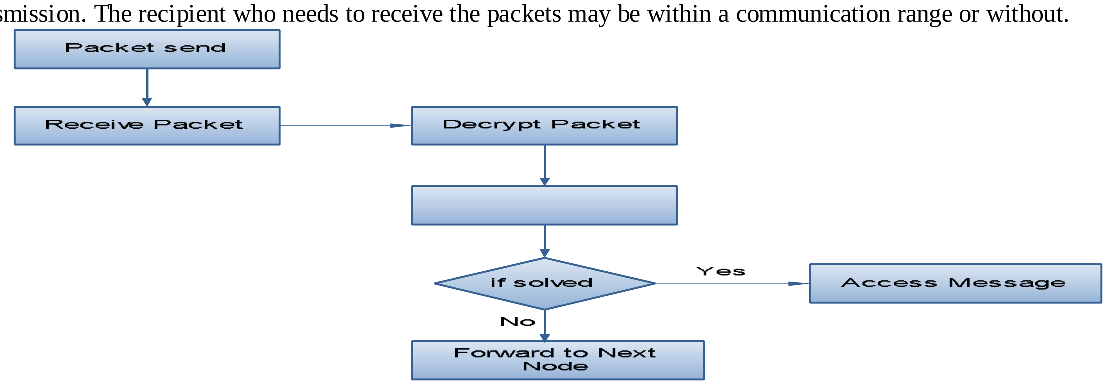

Fig 8. Packet Transmission

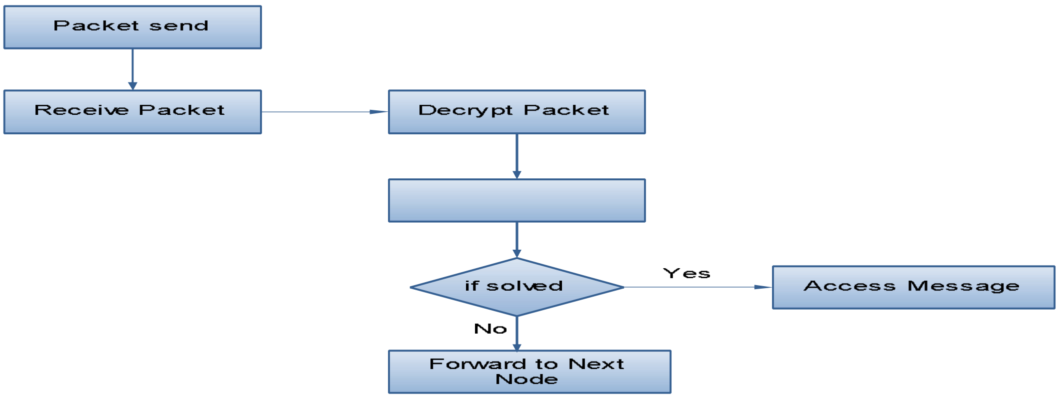

Fig 9.Packet Recovery

The sender sends the packet to the receiver in the communication range directly to the receiver. Otherwise it sends via multi-hop nodes. The key concept is evolved in case to identify the packet which is send by the sender. After identification of the packet the packet gets demodulated i.e. transformed to its original state, de-interleave, and decoded. If the packets get disturbed or if any failure occurs in the transmission of packets the sender resends the packets. The process is named as Packet Recovery.

VII.CONCLUSION

The problem of selective jamming attacks in wireless networks is addressed. An internal adversary model is a model in which the jammer is part of the network under attack, so being aware of the protocol specifications and shared network secrets. To indicate that the jammer can be classified based on the transmitted packets in real time by decoding the first few symbols of an ongoing transmission. The impact of selective jamming attacks on network protocols can be measure by TCP and routing. Particularly the selective jamming attack is selected. The selective jammer can significantly impact performance with very low effort. To discriminate the selective jammers the four schemes are proposed to transform the selective jammer to a random one by preventing real-time packet classification. In this schemes combine cryptographic primitives like as Cryptographic puzzles, commitment schemes and all-or-nothing transformations (AONTs) with physical layer characteristics along with digital signature technique. The security of these schemes is maintained and the quantification is made in computational and communication overhead.

REFERENCES

[1] Alejandro Proan˜o and Loukas Lazos "Packet-Hiding Methods for Preventing Selective Jamming Attacks," IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 1, pp. 101-114, 2012.
[2] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130, 2006.
[3] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.
[4] R.Rivest, A.Shamir, and D.Wagner,"Time-Lock Puzzles and Timed-Release Crypto," technical report, Massachusetts Inst. of Technology, 1996.
[5] W. Xu, W. Trappe, and Y. Zhang, "Anti-Jamming Timing Channels for Wireless Networks," Proc. ACM Conf. Wireless Network Security (WiSec), pp. 203-213, 2008.
[6] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks," Proc. ACM Int'l Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 46-57, 2005.
[7] Y. Desmedt ,"Broadcast Anti- Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.
[8] A. Juels and J. Brainard, " Client Puzzles : A Cryptographic Counter measure against Connection Depletion Attacks," Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999.
[9] R.C. Merkle, "Secure Communications over Insecure Channels," Comm. ACM, vol. 21, no. 4, pp. 294-299, 1978.
[10] D. Stinson , "Something about All or Nothing (Transforms)," Designs, Codes and Cryptography, vol. 22, no. 2, pp. 133-138, 2001.
[11] P. Tague, M. Li, and R. Poovendran, "Mitigation of Control Channel Jamming under Node Capture Attacks," IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221-1234, Sept. 2009.

[12] D. Thuente and M. Acharya, "Intelligent Jamming in Wireless Networks with Applications to 802.11 b and Other Networks," Proc. IEEE Military Comm. Conf. (MILCOM), 2006.

R.Bharathi received her B.E., degree in Computer Science and Engineering from the Anna University, Chennai, India, in 2007, and M.E., degree in Computer Science and Engineering from the Anna University of Technology, Coimbatore, India, in 2009.

She is currently a Professor in the Department of Computer Science and Engineering, in M.Kumarasamy College of Engineering, Karur, Tamil Nadu, India. Her main research interested includes Data structures, networking, wireless networks and mobile computing.

A.Rajesh Kumar received his B.Tech., degree in Information Technology from M.A.M College of Engineering, Tiruchirapalli, India in 2011 and currently doing his M.E., degree from M.Kumarasamy College of Engineering (MKCE), in Computer Science and Engineering respectively.

His research interested focuses on Wireless Networks, Network Security, DoS Attacks in Networks, Selective Jamming attacks and Jamming attacks.