ISSN No. 0976-5697

Volume 5, No. 2, March 2014 (Special Issue)

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Selected Approach for Hiding the Packets from Jamming Attacks

P.Raju
Department of CSE,
SVECW Engg. College,
Affiliated to JNTUK, Bhimavaram, W.G.District,
Pin-534 204, A.P. INDIA,
rajpresy3@gmail.com

R. Shiva Shankar
Department of CSE,
S.R.K.R Engg. College,
Affiliated to Andhra University, Bhimavaram, W.G.District,
Pin-534 204, A.P. INDIA,
shiva.srkr@gmail.com

M. Chilakarao
Department of CSE,
SVECW Engg. College,
Affiliated to JNTUK, Bhimavaram, W.G.District,
Pin-534 204, A.P. INDIA,
chilakarao@gmail.com

Abstract: Jamming attacks are much harder to encounter and have more security problems. They have been shown to actualize severe Denial-of-Service (DoS) attacks in opposition to wireless networks. In the easiest form of jamming, the adversary interferes with the function of messages by broadcasting a constant jamming signal, or many short jamming pulses. Jamming attacks have been measured under an external threat model, wherein the jammer is not part of the network. Under this model, jamming policies include the continuous or casual broadcast of high power interference signals. The nodes to be operate in the conventional relay mode and a number of midway nodes to be broadcasted the signal. The impact of selective jamming attacks is on network protocols like TCP and routing. A selective jammer can considerably impact performance with extremely low effort. We build up three schemes that broadcast a selective jammer to a random one by avoiding real-time packet categorization.

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

I. INTRODUCTION

To build up a competent faster and secure node admission and communications process in Mobile Ad hoc Networks. Client certificates allow for a division of roles which is cannot done by passwords. They do so at the expense of adding a crowd of development and deployment problems which makes them costly. But, passwords stay cheap by fitting in a human brain, which intrinsically implies low security. So the major purpose is to find the correct balance of secure validation in MANETS. The manifestation validates our claim. Usual anti-jamming approaches depend broadly on spread-spectrum (SS) communications or various forms of jamming avoidance SS approaches offer bit-level protection by dispersing bits according to a secret pseudo-noise (PN) code, well-known only to the communicating parties.

These approaches can only care for wireless broadcasting's under the external threat model. Jamming is not a broadcast-only activity. It needs the capability to find out and identify injured network activity, which we indicate as sensing. At the physical layer a sensor required to detect the existence of packets. Because the network is encrypted, only the begin time of the packet and its size can be computed. At superior layers a sensor required to categorize packets using protocol information. Naturally, jamming attacks have been considered under an external threat model, wherein the jammer is not the part of the network. Below this model, jamming techniques include the constant or random broadcast of high-power interference signals. But, accepting an "always- on" technique has different drawbacks. First, the adversary needs to spend a considerable amount of energy to jam frequency bands of curiosity. Second, the constant existence of uncommonly high interference levels makes this type of attacks simple to identify.

a. Fails to effectively treat internal threat models.
b. So the best jamming detection system is needed to handle the internal threat models.

II. LITERATURE SURVEY

A. *Related Work:*

Thuente and Acharya studied the effect of an external selective jammer who aims several control packets at the MAC layer. To complete packet categorization, the adversary utilizes inter packet timing information to deduce reputed packet broadcastings. Upcoming broadcasts at different layers were guessed using predictable timing information. Using their model, the writers proposed selective jamming techniques for famous sensor network MAC protocols.

Constant jamming has been utilized as a denial-of-service (DoS) attack in opposition voice communication since the 1940s [1], [2]. Currently, different alternative jamming approaches have been established [4], [5]. Intelligent attacks which aim the broadcast of definite packets were offered in [3]. Selectivity was attained by inference from the control messages already broadcasted. Channel-selective jamming attacks were presented in [3]. It was shown that aiming the control channel decreases the

CONFERENCE PAPER
Two day National Conference on Advanced Trends and Challenges in Computer Science and Applications
Organized by: Shree Vishnu Engineering College for Women, Bhimavaram A.P.
Schedule: 18-19 March 2014

needed power for completing a denial- of- service attack by different orders of magnitude.

WLAN Client-Server & Ad-Hoc Network

Because WLAN offers users the mobility to go around inside the local area exclusive of a wire and still join to the network, it is broadly used in several significant areas. Banks, governments, corporations, and institutions pass the extremely significant data via WLANs. The security issues of WLANs become essential for the users. The majority of WLANs are according to the IEEE 802.11 standard that broadcast data in many channels depending on frequencies. Because installation and convenience is simple, WLAN is frequently used in everyday life [6]. An beginning of WLANs was completed by Gast (2005) and Mark (2005). By using Receiver Operating Characteristics (ROC) on nodes, DoS 8 attacks can be guessed by preparing the categorization of jammers under several attack situations. Research in this thesis was centered on two kinds of WLANs: client-server and ad-hoc networks.

a. Jamming Attacks:

The DNS is a hierarchical tree organization whose root node is well-known as the root domain. A label in a DNS name in a straight line corresponds with a node in the DNS tree organization. A label is an alphanumeric string that individually recognizes that node from its siblings. Labels were written from left to right.

Only one zero length labels are permitted and are kept for the root of the tree. Because WSNs are utilized in observing medical uses, homeland security, industrial automation, and military applications, security of WSNs be required to be guaranteed. Overcoming various threats of DoS attacks on WSNs is done by encryption and confirmation, but a few other approaches still required to be found to stop from particular DoS attacks, mainly Denial of Sleep attacks, those are critical threats in WSNs still.

b. Detection of Jamming:

WLANs are developed upon a shared medium that does it simple to initiate jamming attacks. These attacks can be simply established by transferring radio frequency signals that do not go behind any of the MAC protocols. Identification of jamming attacks can be completed in several ways. One of the main effective means is to jump channels. Since contact between two valid nodes is done through a particular frequency, the frequency can be altered if compulsory.

When the nodes identified the jamming in the wireless network, they jumped to some other channel to carry on valid communication. After channels were flying the network continue communications as usual. In both the situations, the amount of packets dropped decreased instantaneously.

The conclusion of the research is that channel jumping will in turn reduces the throughput of the network. Also, it was simple to identify jamming through intermitted channel jumping. Cross-layer jamming identification is a tree-based method. A jamming detection algorithm was used in all the valid nodes; when the communication process start, all the nodes had the capability to report jamming attacks in several layers, and only the reports which were produced by nodes by jamming detection algorithm were received by the system in order to escape error. Research was also complete about multi-channel jamming attacks by Jiang and Xue (2010). The variation from the jamming detection algorithm was that it centered on network restoration and design of traffic rerouting.

B. Modules:

a. Real Time Packet Classification
b. A Strong Hiding Commitment Scheme
c. Cryptographic Puzzle Hiding Scheme
d. Hiding based on All-Or-Nothing Transformations

III. ARCHITECTURE

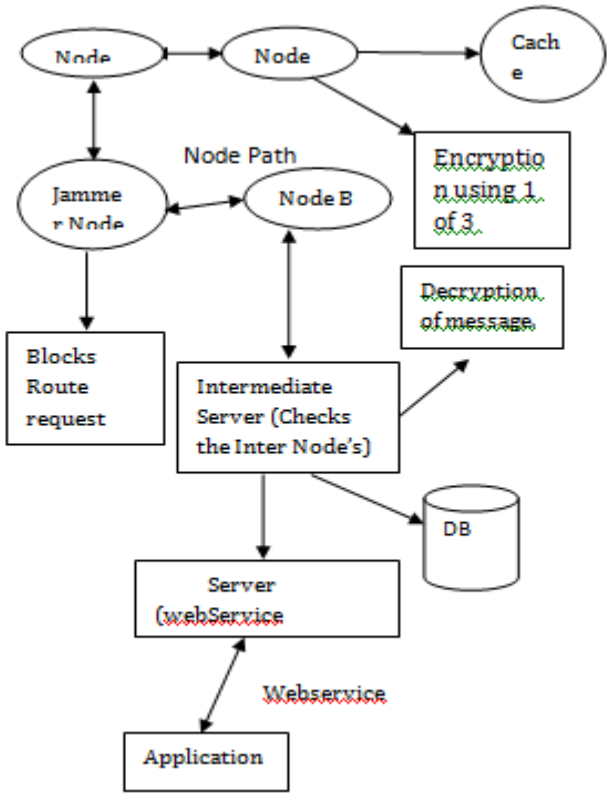


Figure: 1

A. Modules Description:

a. Real Time Packet Classification:

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is passed above the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to get better the actual packet m. Nodes A and B commune through wireless connection. Surrounded by the broadcast range of both A and B there is a jamming node J. When A passed a packet m to B, node J categorizes m by getting only the first little bytes of m. J then alters m beyond recovery by intrusive with its reception at B.

b. A Strong Hiding Commitment Scheme:

A well-built hiding promise scheme (SHCS) that is according to symmetric cryptography. Suppose that the sender has the packet for Receiver. First, S prepares commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a widely called as permutation, and k is a by chance selected key of some wanted key length s (the length of k is a security parameter). Upon reception of d, any receiver computes R.

CONFERENCE PAPER
Two day National Conference on Advanced Trends and Challenges in Computer Science and Applications
Organized by: Shree Vishnu Engineering College for Women, Bhimavaram A.P.
Schedule: 18-19 March 2014

c. Cryptographic Puzzle Hiding Scheme:

A sender S has a packet m for broadcasting. The sender picks a random key k , of the required length. S produces a puzzle (key, time), where puzzle () indicates the puzzle generator function, and tp indicates the desired time for the answer of the puzzle. Parameter is computed in the units of time, and it is openly reliant on the unspecified computational ability of the adversary, indicated by N and computed in computational operations per second. After producing the puzzle P, the sender transmits (C, P). At the receiver side, any receiver R answers the received puzzle to get better key and then measures.

d. Hiding based on All-Or-Nothing Transformations:

Before broadcasting the packets are pre-progresses by an AONT but stay unencrypted. The jammer cannot complete packet categorization until all pseudo-messages matching to the actual packet have been obtained and the inverse alteration has been applied. Packet m is divided into a group of x input blocks m = {m1, m2, m3….} that provided as an input. The group of pseudo-messages m = {m1, m2, m3,…..} is broadcasted above the wireless medium.

B. Algorithm:

a. Symmetric encryption algorithm
b. Brute force attacks against block encryption algorithms.

We propose a solution based on All-Or- Nothing Transformations (AONT) that initiate a modest broadcasting and computation overhead. Such transformations were actually proposed by Rivest to slow down brute force attacks in opposition block encryption algorithms. An AONT provided as a widely known and totally invertible pre-processing step to a plaintext before it is transmitted to an normal block encryption algorithm

a. Algorithm Description:

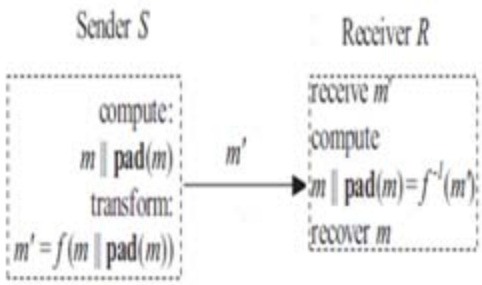


Figure: 2

The Package Transform- In the package transforms the specified a message m, and the random key ḱ, the output pseudo-messages are calculated as follows:

$$m'_i = m_i \oplus E_{k'}(i), \text{ for } i=1,2,3\ldots\ldots,x$$

$$m'_{x+1} = k' \oplus e_1 \oplus e_2 \oplus e_3 \oplus \ldots\ldots\ldots\ldots \oplus e_x,$$

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

$$k' = m'_{x+1} \oplus e_1 \oplus e_2 \oplus e_3 \oplus \ldots\ldots\ldots\ldots \oplus e_x,$$

$$m_i = m'_i \oplus E_{k'}(i), \text{ for } i=1,2,3\ldots\ldots,x,$$

Note that if any m'i is not known, any value of ḱ is probable, because the equivalent e_i is not known. Hence, Ek' (i) cannot be get back for any i, making it infeasible to get any of the m_i .

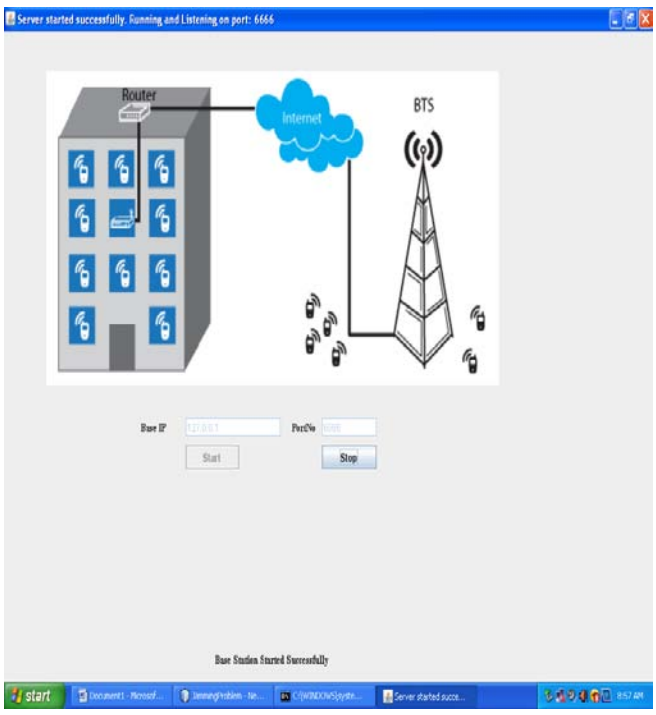
C. Hiding Sublayer Details:

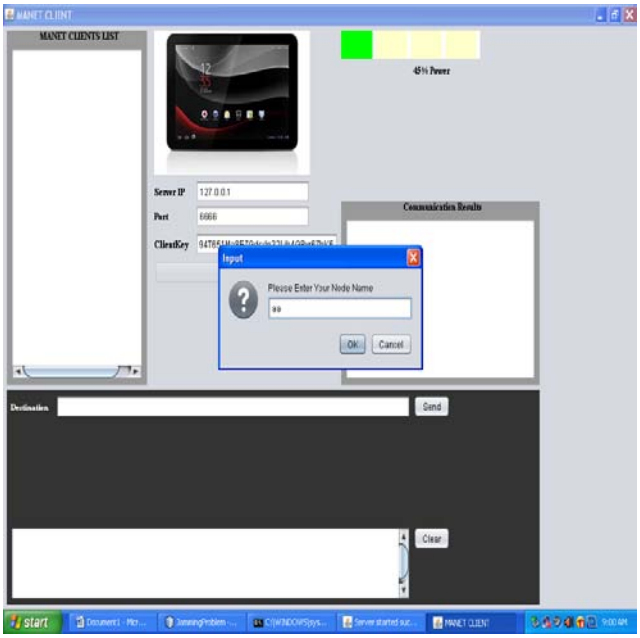
AONT-HS is developed at the hiding sublayer exist in between the MAC and the PHY layers. In the beginning, m is padded by applying the function pad() to alter the frame length so that no padding is required at the PHY layer, and the length of m becomes a numerous of the length of the pseudo-messages m′ i. This will make sure that all the bits of the broadcasted packet are the part of the AONT. In the subsequent step, m||pad(m) is divided to x blocks, and the AONT f is applied. Message m′ is reached to the PHY layer. At the receiver, the reverse transformation f−1 is applied to get m||pad(m).

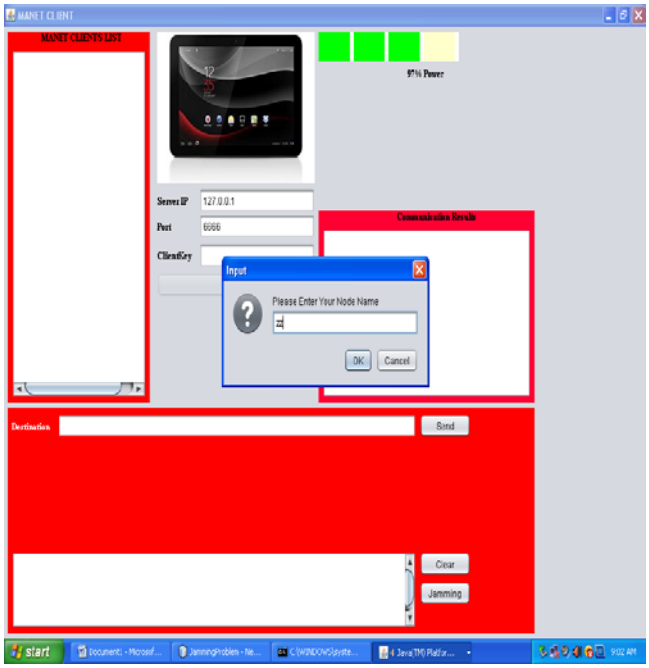
IV. RESULTS

The performance of the policy assessment method in MController, it altered the number of the controllers of a shared photo from 1 to 5, and allotted every controller with an average number of friends, 20, which is maintained by Face book figures. Also, it considered two cases for our evaluation. In completed 100 individual trials and computed the significance of every trial. Since the system performance bases on the remaining processes running at the time of computation, it had early inconsistencies in this performance. To reduce such an effect, it completed 10 separate trials (a total of 100 calculations for each number of controllers).

For both the cases, the investigational results visualized in Fig 4.1 and Fig 4.2 that the policy evaluation time enhances in early with the raise of the number of controllers. With the easiest development of this mechanism, where n is the quantity of controllers of a shared photo, a sequence of operations basically takes place n times. Furthermore, it could examine there was no important overhead when it run MController in Face book.







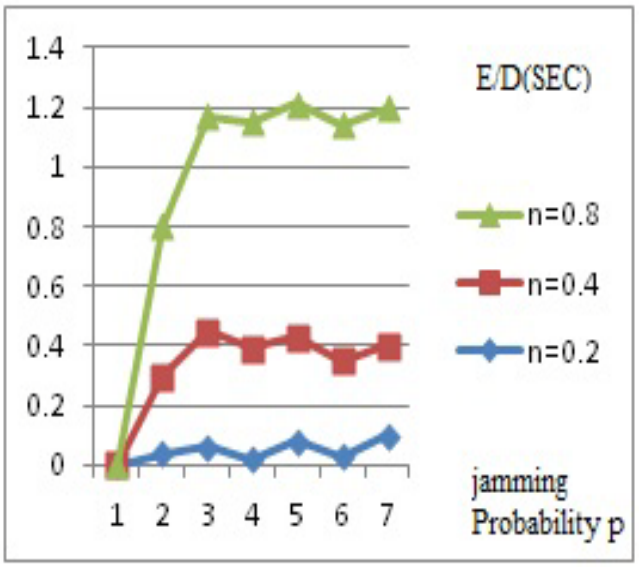


Figure 4.1 Average Application Delay [E/D]

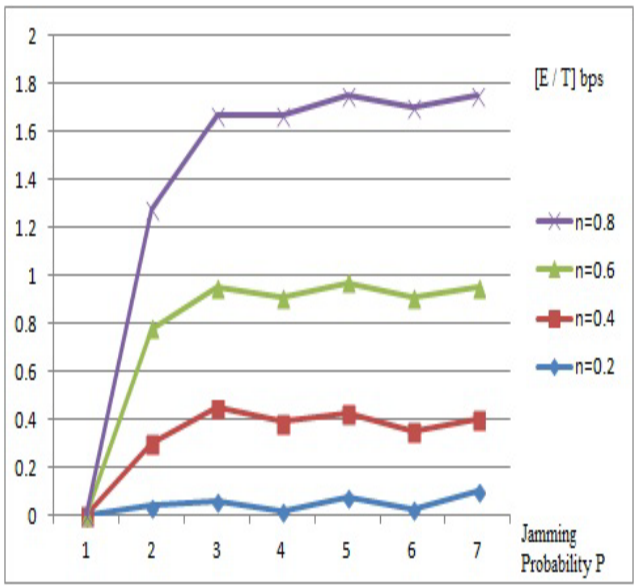


Figure 4.2 Average Effective Throughput E[T]

V. CONCLUSION

An internal adversary model, in which the jammer is a part of the network under the attack, therefore being aware of the protocol requirements and shared network secrets. We demonstrated that the jammer can categorize the broadcasted packets in real time by decoding the first little symbols of a continuing transmission. We assessed the effect of selective jamming attacks on network protocols like TCP and routing. Our findings demonstrate that a selective jammer can importantly impact performance with extremely low effort. We implemented three schemes that broadcast a selective jammer to a random one by stopping real-time packet categorization.

Jamming attack is a type of Denial of Service (DOS) attack, which stops other nodes from using the channel to contact by engaging the channel that they are contacting on. To stop such attack, we propose a packet approach based on All-or-Nothing Transform (AONT). An AONT itself does not complete any encryption, because there is no secret key data involved in it. However, if its outcome is encrypted, block- by- block, with a block cipher, the resultant scheme will have the subsequent exciting property- one have to decrypt the whole cipher text prior one can determine even one message block.

VI. REFERENCES

[1]. Mario cagalj, srdjan capkun, jean hubaux, “Wormhole-Based Antijamming Techniques in Sensor Networks”, ieee transactions on mobile computing, vol. 6, no. 1, 2007.

[2]. Wenyuan Xu , Wade Trappe, Yanyong Zhang, “Channel Surfing: Defending Wireless Sensor Networks from Interference”, USA, IPSN', 2007.

[3]. Wenyuan Xu , Wade Trappe, Yanyong Zhang, “Anti-jamming Timing Channels for Wireless Networks”, USA, WiSec, 2008.

[4]. Alejandro Proano and Loukas Lazos. “Packet-Hiding Methods for Preventing Selective Jamming Attacks”. IEEE Transactions on dependable and secure computing, Vol. 9, No. 1, 2012.

[5]. C. Po¨pper, M. Strasser, and S. C˘ apkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.

[6]. 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 Sensor Networks, 5(1):1–38, 2009.

[7]. M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders. "Reactivejamming in wireless networks: How realisticis the threat?" InProceedings of WiSec, 2011.

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