Anti-Jamming Schemes To Prevent Selective Jamming Attacks

Ramesh Kande[#1], B.Madhura Vani[*2]

[#1]M.Tech, Computer Science Engineering, MLRIT, Hyderabad, Andhra Pradesh, India
[#2]Assistant Professor, Department of CSE, MLRIT, Hyderabad, Andhra Pradesh, India

Abstract--Wireless networks are more vulnerable to interference attacks as they are open in nature. These attacks are also known as Denial-of-Service attacks that cause some sort of jamming in the network. Jamming problem has been around in wirelessnetworks. Many existing solutions to prevent jamming attacks employed external threat model. However, there is possibility of internal attacks. Adversaries with good knowledge of network details including protocol specifications and other secret can make jamming attacks that are not easy to handle. Such attacks are named as selective jamming attacks as they are active for very short span of time that focus on messages with highest significance. Recently Proan˜o and Lazos proposed an internal threat model to handle selective jamming attacks. They also provided three schemes for preventing selective jamming attacks. In this built a prototype application in Java platform to implement the schemes for preventing selective jamming attacks. Experimental results revealed that the prototype can be used in real world wireless networks.

Index Terms –Wireless networks,selective jamming attacks, packet classification

I. INTRODUCTION

Networks without physical cables became popular. Such networks are open in nature. Jamming in wireless networks can disrupt normal communication. Two nodes in wireless network need full availability of wireless medium for proper communication. The participating nodes cannot communicate meaningfully when the wireless medium is interrupted by adversaries by launching Denial-of-Service attacks (DoS). Many DoS attacks were reported in the literature in [1], [2], [3] and [4]. These attacks are jamming attacks that disrupt services between wireless nodes to eavesdrop the communications over wireless networks. Jamming attacks are made in wireless networks by adversaries by continuously sending signals to deny normal service between the nodes.

Many researchers considered external threat model to solve jamming attacks. In the external threat models, the jammers are not included as part of network. In this threat model the adversaries continuously send high power signals inorder to disrupt normal communications between wireless nodes. This kind of jamming attacks is also known as DoS [2], [5]. This attack can be identified and prevented with relative ease when compared with internal jamming attacks. This is for because the adversary has to interfere the network continuously that makes it easy to detect. Spread-spectrum (SS) communications is used for traditional antijamming techniques [5].

Recently Proan˜o and Lazos [6] proposed a packet hiding methods to prevent selective jamming attacks. They considered internal threat model where an adversary is expected to have knowledge of network and perform interference attacks for short span of time. That too the adversaries are assumed to target only messages of high importance. They follow the concept of classify the packets and then jam.

Classifying packets and [7], [8] and decoding packets [9] are the strategies used by adversaries for selective jamming attacks. Proan˜o and Lazos [6] provided packet hiding methods to prevent selective jamming attacks.

In this paper we implement the selective jamming methods proposed by Proan˜o and Lazos [6] using Java platform. We built a prototype that demonstrates the proof of concept. The remainder of this paper is structured as follows. Section II reviews literature pertaining to jamming attacks and selective jamming attacks. Section III presents proposed problem statement and threat model. Section IV provides packet classification in real time. Section V presents packet hiding methods. Section VI provides information about prototype implementation. Section VII presents experimental results while section VIII concludes the paper.

II. PRIOR WORKS

This section provides review of literature pertaining to jamming attacks and their prevention methods.Jamming attacks have been around since 1940s [5]. Studies on controllingpackets at MAC layer was carried out in [33]. Inter-packet timing information is exploited by adversaries for packet classification. Later on researchers focused on selective jamming attacks on MAC protocols of sensor networks. The feasibility of selective jamming attacks is illustrated in [8]. Unification of packet characteristics and packet classification were focused in [10]. In [11] SPREAD system was proposed to prevent smart jamming. A wireless protocol which is similar to 802.11 was presented by Greenstein et al. to prevent classification of attacks. All explicit identifiers are hidden by the protocol [12]. Software defined radio engines [9], [13] are also used to implement selective jamming attacks. USRP2-based jamming solution was explored by Wilhelm et al. which were for both selective and reactive jamming attacks. It was found in the literature that 99.96 percent is the success rate of selective jamming when experiments are made with 802.15.4. With selective jamming, rate of communication comes down in wireless network.

Many researchers studied on channel-selective jamming attacks. They reduce the power required by DoS attacks [14]. The solution for this problem was given by [15], [16], and [8]. A randomized frequency hopping method is used to prevent such attacks. Antijamming technique for such attacks also presented by Strasser et al. [17]. Non selective jamming attacks are also found in literature. SS communications [5], [18] were used by conventional methods for preventing jamming attacks. A communication mode which is jamming-resistant was proposed by Popper et al. This technique does not depend on the concept of shared secrets. In this technique UDSSS is used for physical layer modulation. A broadcast method for anti jamming was also proposed in [19]. ECC capabilities were explored by [1], and [20]. They classified it into four modules. They are constant jammer, deceptive jammer, random jammer, and reactive jammer.

III. PROBLEM STATEMENT AND THREAT MODEL

The proposed solution is based on the schemes presented by Proan˜o and Lazos [6] for selective jamming attacks. The problem of selective jamming attacks is illustrated in figure 1. The realization of the selective jamming attacks is visualized in the figure.

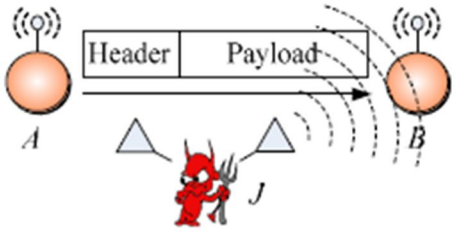

Fig. 1 –Illustrates selective jamming attack (excerpt from [1])

As can be seen in fig. 1, it is evident that there is selective jamming attack launched by internal adversary who has the knowledge of network and underlying protocol specifications besides secrets. The adversary also targets the messages of high importance. The attack is made selectively and for very short span of time.

Threat Model

The proposed threat model is an internal model where adversaries are aware of underlying network and protocols. The adversaries also have the knowledge of the time in which high importance messages travel between specific nodes. Based on this knowledge only the adversaries perform such attacks for very short span of time making it difficult to detect the jamming attack.

IV. REAL TIME PACKET CLASSIFICATION

In case of selective jamming attacks, the adversaries are capable of classifying packets on the fly. After classifying packets, adversaries can easily take decisions for selective jamming attacks and the highly important content. It is done in the physical layer. Figure 2 illustrates general communication mechanism which is known to adversaries.

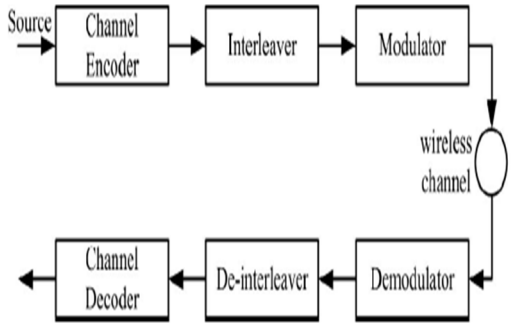

Fig. 2 –General communication mechanism

V. PROTOTYPE IMPMPLEMENTATION

This section provides details about the environment used for application development, the results and comparison of the proposed scheme with existing scheme. The environment used is a PC with 2 GB RAM with Core 2 Duo processor. The software includes JDK 1.6, and NetBeans. NetBeans is an Integrated Development Environment (IDE) used for rapid application development.

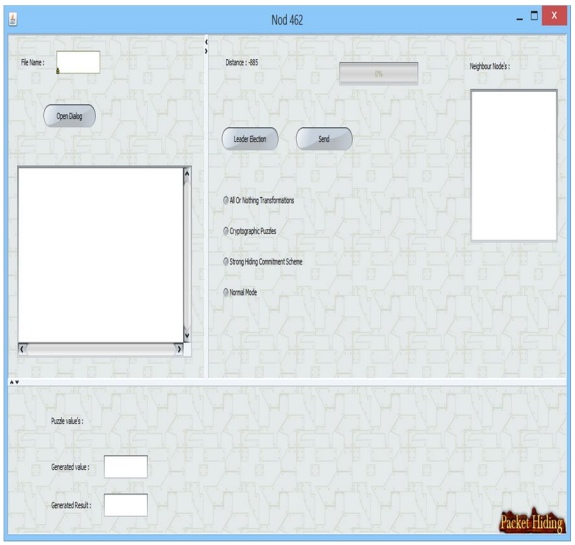

Fig 3 First Node

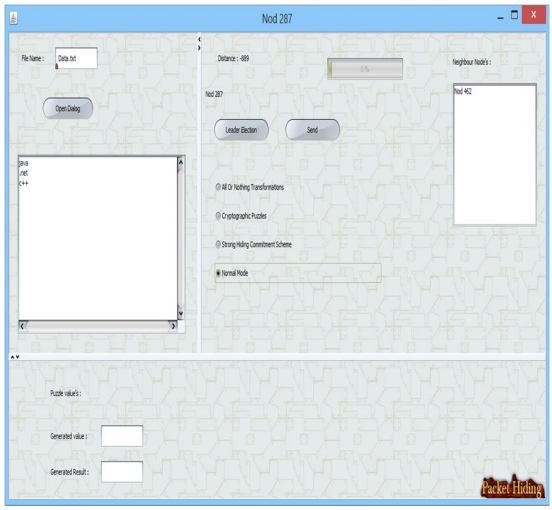

Fig 4 Second Node

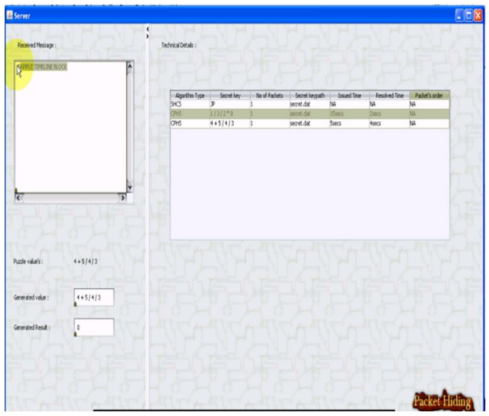

Fig 5 Server

EXPERIMENTAL RESULTS

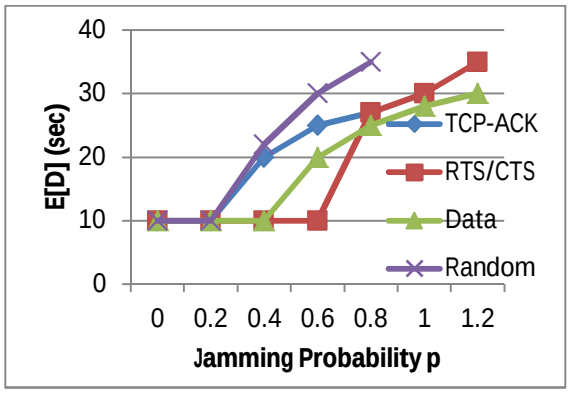

Fig 6 Average application delay E [D].

As shown in the above figure 3 represents horizontal axis represents jamming probability while vertical axis represents E[d].

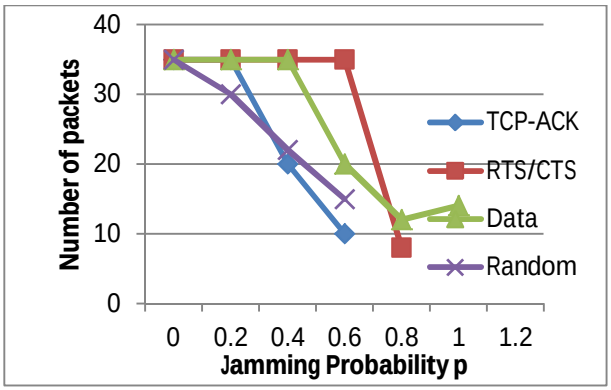

Fig 6 Average effective throughput E [D].

As shown in the above figure 4 represents horizontal axis represents jamming probability while vertical axis represents number of packets.

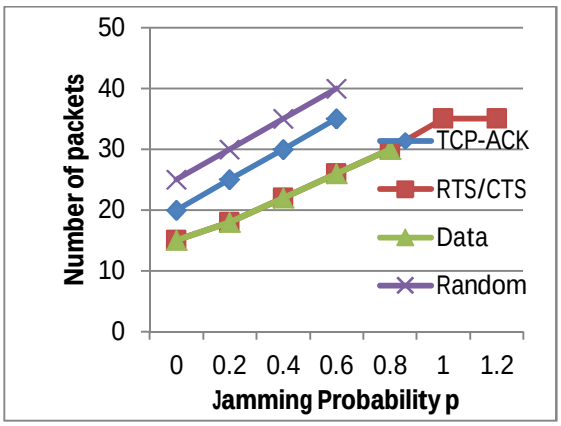

Fig 7 Number of packets jammed

As shown in the above figure 5 represents horizontal axis represents jamming probability while vertical axis represents number of packets.

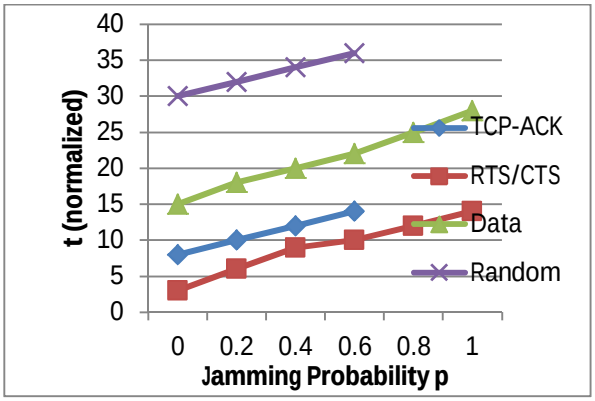

Fig 8 Fraction of time the jammer is active.
As shown in the above figure 6 represents horizontal axis represents jamming probability while vertical axis represents t normalized.

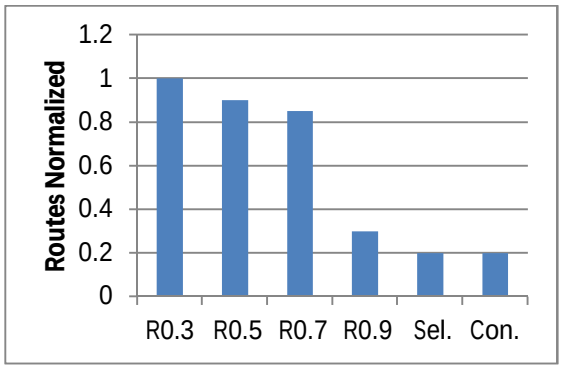

Fig 9 Number of connections established in the network.

As shown in the above figure 4 represents the vertical axis represents routes normalized.

VI. CONCLUSION

In this paper, we have implemented anti-jamming schemes to prevent selective jamming attacks. The schemes were proposed by Proan˜o and Lazos [6]. We built a prototype application that demonstrates proof of concept pertaining to selective jamming attacks. Many existing techniques focused on external threat model on jamming attacks. In this paper we considered the selective jamming attacks launched by adversaries who have knowledge of the network and underlying protocol specifications. The jamming attack is made selectively for very short span of time targeting highly important messages. The adversaries need less effort to perform selective jamming attacks. Such attacks can't be easily detected. However the prototype demonstrates the effectiveness of the schemes implemented to prevent selective jamming attacks. The empirical results revealed that the prototype is useful in real time applications.

REFERENCES

[1] W. Xu, T. Wood, W. Trappe, and Y. Zhang, "Channel Surfing andSpatial Retreats: Defenses against Wireless Denial of Service,"Proc. Third ACM Workshop Wireless Security, pp. 80-89, 2004.

[2] W. Xu, W. Trappe, Y. Zhang, and T. Wood, "The Feasibility ofLaunching and Detecting Jamming Attacks in Wireless Networks,"Proc. ACM Int'l Symp. Mobile Ad Hoc Networking andComputing (MobiHoc), pp. 46-57, 2005.

[3] G. Noubir and G. Lin, "Low-Power DoS Attacks in Data WirelessLans and Countermeasures," Mobile Computing and Comm. Rev.,vol. 7, no. 3, pp. 29-30, 2003.

[4] L. Lazos, S. Liu, and M. Krunz, "Mitigating Control-ChannelJamming Attacks in Multi-Channel Ad Hoc Networks," Proc.Second ACM Conf. Wireless Network Security, pp. 169-180,
2009.

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

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

[7] T.X. Brown, J.E. James, and A. Sethi, "Jamming and Sensing ofEncrypted Wireless Ad Hoc Networks," Proc. ACM Int'l Symp.Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130,2006.

[8] M. Wilhelm, I. Martinovic, J. Schmitt, and V. Lenders, "ReactiveJamming in Wireless Networks: How Realistic Is the Threat," Proc.ACM Conf. Wireless Network Security (WiSec), 2011.

[9] 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, JANUARY/FEBRUARY 2012.

[10] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.

[11] X. Liu, G. Noubir, and R. Sundaram, "Spread: Foiling Smart Jammers Using Multi-Layer Agility," Proc. IEEE INFOCOM, pp. 2536-2540, 2007.

[12] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall, "Improving Wireless Privacy with an Identifier-Free Link Layer Protocol," Proc. Int'l Conf. Mobile Systems, Applications, and Services (MobiSys), 2008.

[13] B. Thapa, G. Noubir, R. Rajaramanand, and B. Sheng, "On the Robustness of IEEE802.11 Rate Adaptation Algorithms against Smart Jamming," Proc. ACM Conf. Wireless Network Security (WiSec), 2011.

[14] 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.

[15] 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.

[16] P. Tague, M. Li, and R. Poovendran, "Probabilistic Mitigation of Control Channel Jamming via Random Key Distribution," Proc. IEEE Int'l Symp.Personal, Indoor and Mobile Radio Comm. (PIMRC), 2007.

[17] M. Strasser, C. Po¨pper, and S. _Capkun, "Efficient Uncoordinated fhss Anti-Jamming Communication," Proc. ACM Int'l Symp.Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 207-218, 2009.

[18] Y. Desmedt, "Broadcast Anti-Jamming Systems," Computer Networks, vol. 35, nos. 2/3, pp. 223-236, Feb. 2001.

[19] C. Po¨pper, M. Strasser, and S. _Capkun, "Jamming-Resistant Broadcast Communication without Shared Keys," Proc. USENIX Security Symp., 2009.

[20] G. Lin and G. Noubir, "On Link Layer Denial of Service in Data Wireless LANs," Wireless Comm. and Mobile Computing, vol. 5, no. 3, pp. 273-284, May 2004.

Authors

K.Ramesh, he is pursuing M.Tech (CSE) in MLRIT, Hyderabad, AP, INDIA. He has received B.Tech degree in Computer Science and Engineering. His main research interest includes Networking and Ethical Hacking.

B. Madhuravani, Asst.Prof, Department of CSE, MLR Institute of Technology, Dundigal, Hyderabad. She is doing Ph. D in Computer Science & Engineering, JNTUH. Her research interests include Information Security, Computer Networks, Distributed Systems and Data Structures.