IJCSE International Journal of Computer Sciences and Engineering Open Access
Research Paper Vol.-7, Issue-5, May 2019 E-ISSN: 2347-2693

Defeating Jamming Attack in Wireless Network Techniques

T.Aruna[1*], R. Anandha Jothi[2], V. Palanisamy[3]

[123] Department of Computer Applications, Alagappa University, Karaikudi, India

Corresponding Author: aruna1995mca@gmail.com

DOI: https://doi.org/10.26438/ijcse/v7i5.13841388 | Available online at: www.ijcseonline.org

Accepted: 26/May/2019, Published: 31/May/2019

Abstract— The open nature of the wireless form leaves it vulnerable to intentional interference attacks, typically referred to as jamming. This intentional intrusion with wireless transmissions can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks. Typically, jamming has been addressed under an external threat representation. However, adversaries with internal knowledge of protocol description and network secrets can launch low-effort jamming attacks that are difficult to recognize and counter. In this work, we address the issue of selective jamming attacks in wireless networks. In these attacks, the opponent is active only for a short period of time, selectively targeting messages of high importance. We embellish the advantages of selective jamming in terms of network staging mortification, and opponent effort by presenting two case studies; a selective pounce, on TCP and one on routing. We show that selective jamming attacks can be launched by execute real-time packet classification at the physical layer. To mitigate this pounce, we develop three schemes that intercept real-time packet classification by combining cryptography primitives with physical-layer attributes. We inspect the security of our procedure and evaluate their computational and communication overhead.

Keywords— *Jamming, Attack, Network, Defective*

I. INTRODUCTION

Wireless networks rely on the untroubled, availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security ultimatums. Anyone with a transceiver can intrude on wireless transmissions, administer specious messages, or jam legitimate ones [1]. While intrude 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 opposition wireless networks [2, 3]. In the uncomplicated form of jamming, the opponent obstruct with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses. 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 scheme includes the continuous or random transmission of high-power intrusion signals [4]. 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.

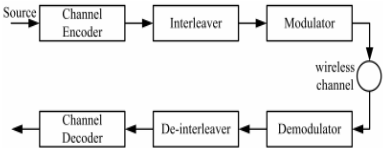

Figure.1. Communication System

Second, the continuous existence of unusually high intrusion levels makes this type of attacks easy to recognize. 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 contribute bit-level protection by spreading bits according to a Secret Pseudo-Noise (PN) code, known only to the communicating parties [5]. These methods can only protect wireless transmissions under the external ultimatum model. Potential declaration of secrets due to node compromise neutralizes the gains of SS [6, 7]. 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 cryptography information. In this paper, we address the problem of jamming under an internal ultimatum model. We consider a experienced, adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack.

The opponent utilizes his internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted [8]. For example, a jammer can target route-request/route-reply messages at the routing layer to intercept route learning, or quarry TCP concession in a TCP session to seriously reduce the throughput of an end-to-end flow. To launch selective jamming attacks, the opponent must be capable of implementing a "classify-then-jam" procedure before the completion of a wireless transmission[9]. Such strategy can be actualized either by classifying dispatch packets using protocol semantics, or by decoding packets on the fly. In the latter method, the jammer may decipher the first few bits of a packet for improve useful packet identifiers such as packet type, source and destination address. After classification, the opponent must induce a sufficient number of bit errors so that the packet cannot be improved at the receiver. Selective jamming necessary an confidential knowledge of the Physical (PHY) layer, as well as of the specifics of upper layers [10].

II. RELATED WORK

Jamming attacks on voice communications have been instigate since the 1940s. In the background of digital communications, the jamming problem has been addressed under various ultimatum models. We present a classification based on the selective nature of the adversary.

1) Prior work on Selective Jamming

B. MAC layer

Thuente knowing the impact of an external selective jammer who targets various control packets at the MAC layer[11]. To perform packet classification, the opponent exploits inter-packet timing information to infer illustrious packet transmissions. In Law et al. proposed the estimation of the expectation dispensation of inter-packet transmission times for different packet types based on network traffic analysis. Future transmissions at various layers were predicted using evaluate timing information.

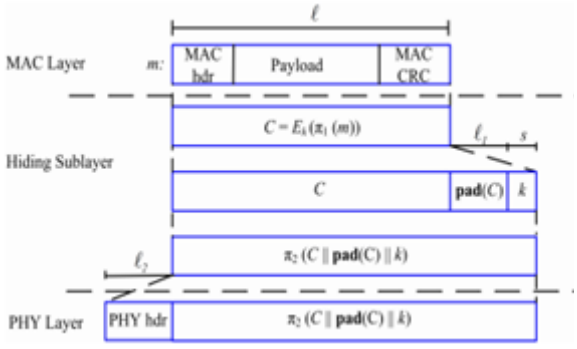

Figure 2. Mac Layer

C. Jamming Strategies

Using their model, the reporter proposed selective jamming strategies for well known sensor network MAC protocols. In, Brown et al. illustrated the achievability of selective jamming based on protocol semantics [12]. They considered several packet identifiers for encrypted packets such as packet size, precise timing information of dissimilar protocols, and physical signal sensing. To intercept selectivity, the integration of packet characteristics such as the least length and inter-packet timing was proposed [13]. Similar packet classification techniques were analysing in. Liu et al. considered a smart jammer that takes into account protocol specifics to optimize its jamming procedure [14]. The adversary was assumed to target control messages at different layers of the network stack [15]. To mitigate smart jamming, the authors proposed the SPREAD system, which is based on the idea of stochastic selection between collections of parallel protocols at each layer. The uncertainty introduced by this stochastic selection, mitigated the selective ability of the jammer. Greenstein et al. presented a 802.11-like wireless protocol called Slyfi that intercept the classification of packets by external viewers. This protocol hides all explicit identifiers from the transmitted packets by encrypting them with keys only known to the intended receivers [25, 26, and 27].

Selective jamming attacks have been experimentally executed using software-defined radio engines. Wilhelm et al. executed a USRP2-based jamming platform called RFReact that enables selective and reactive jamming. RFReact was shown to be agnostic to technology standards and readily flexible to any desired jamming strategy.

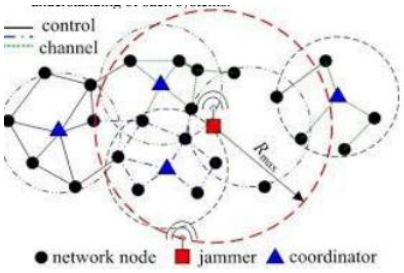

Figure 3. Jamming Architecture

Selective jamming attacks against the rate-adaptation contrivance of 802.11. They showed that a selective jammer targeting specific packets in a point-to point 802.11 conveyance was able to decrease the rate of the communication to the least value of 1 Mbps, with relatively little attempt[16,17]. The consequence was experimentally verified using the USRP2/GNU radio platform.

Assorted researchers have suggested channel-selective jamming attacks, in which the jammer targets the broadcast control channel. It was shown that such attacks reduce the

required power for performing a DoS attack by several orders of magnitude. To protect control-channel traffic, the replication of control transmission in multiple channels was proposed in. The "locations" of the control channels where cryptographically protected. In, Lazoset al. proposed a randomized frequency hopping instructions to protect the control channel from interior jammers. Strasser et al. proposed a frequency hopping anti-jamming technique that does not require the existence of a secret hopping sequence, shared between the communicating parties.

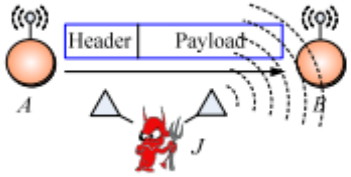

Figure 4. Jamming Attack

D. Jamming Attacks

The success rate of a selective jamming pounce against a 802.15.4 network was measured to be 99.96%. Blapa et al. cstudied

2) Non-Selective Jamming Attacks

A. Broadcast Communications

Conventional procedure for mitigating jamming employs some form of SS conveyance. The transmitted signal is spread to a huge bandwidth following a PN sequence [18]. Without the knowledge of this sequence, a large amount of energy (typically 20-30 dB gain) is required to interfere with an on-going transmission [19]. However, in the case of broadcast communications, compromise of commonly shared PN codes neutralizes the advantages of SS.

B. Uncoordinated Direct Sequence Spread Spectrum

Popper et al. initiate a jamming-resistant communication model for pairwise communications that does not rely on shared secrets [20]. Communicating nodes use a physical layer modulation procedure called Uncoordinated Direct Sequence Spread Spectrum (UDSSS). They also initiate a jamming-resistant broadcast method in which transmissions are spread according to PN codes randomly selected from a general codebook. Several other projects remove overall the need for secret PN codes.

3. Wormhole-based ant jamming techniques in sensor networksA. Denial-of-Service

Due to their very nature, wireless sensor networks are possibly the category of wireless networks most endangered to "radio channel jamming"-based Denial-of-Service (DoS) pounce. An opponent can easily mask the events that the sensor network should detect by stealthily jamming an appropriate subset of the nodes; in this way, he prevents them from reporting what they are sensing to the network operator. Therefore, even if an event is discern by one or several nodes (and the sensor network is otherwise fully connected), the network operator cannot be enlightened on time [21, 22]. We show how the sensor nodes can utilize channel diversity in order to create wormholes that lead out of the jammed region, through which an alarm can be dispatch to the network operator [23, 24]. We propose three solutions: The first is based on wired pairs of sensors, the second relies on frequency hopping, and the third is based on a novel concept called uncoordinated channel hopping. We develop suitable mathematical models to study the suggested solutions.

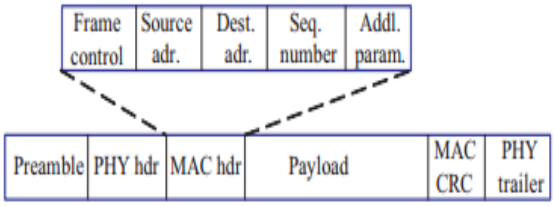

Figure 5. Wireless Network

4) Control channel jamming: Resilience and identification of traitors

A. Channel Jamming

We address the issue of countering the control channel jamming in wireless communication systems. Targeting control traffic on a system like GSM (e.g., BCCH channel) leads to smart attacks that are four orders of vastness more efficient than blind jamming[28,29,30]. We propose several schemes based on coding theory and its applications that can counter both external and internal attackers (traitors)[31,32,33]. We introduce a T-(traitor) resilient scheme that requires less than control information retransmissions and guarantees delivery of control information against any coalition of traitors. The proposed scheme also allows the identification of the traitors[34,35].

III. RESULTS AND DISCUSSION

In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated that is aware of network secrets and the implementation details of networks 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.

Algorithm	No. of Hops	Metrics	Find Jamming Attack	Open Issues
Multi-terminal covert timing channels	Multi	Speed	Periodic	Transmissio n
Wireless communication scheme	Multi	Direction	-	High mobility
Stackelberg Equilibrium (SE)	Two	Mobility	Periodic	High overhead
Uncoordinated Spread Spectrum (USS) technique	Two	Speed	Periodic	High mobility
Energy-constrained jamming systems	One	Location	Periodic	High cost
Timing-Channel Aloha	Multi	Direction	Periodic	Location accuracy
OPNET 11.5	Multi	Location	--	Design of OPNET
IEEE802.11 rate adaptation algorithms (RAA)	Multi	Speed	--	Network topology
GUIDE algorithm	Multi	Mobility	--	--
Uncoordinated frequency hopping (UFH) scheme	Two	Direction	Periodic	Network stability
Distributed Denial of Service (DDoS)	Two	Location	Periodic	High overhead
Information-centric Internet architecture	Two	Speed, Location	Periodic	Location accuracy
Named data networking	Two	Mobility	--	Network stability
Bloom-filter-based forwarding	Two	Speed, Location	Periodic	Faulty affiliation
Timely Estimation of Traffic Matrices	Multi	Location, direction	Periodic	High overhead

IV. CONCLUSION AND FUTURE SCOPE

We addressed the issue of selective jamming pounce in wireless 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 showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an on-going transference. We appraised the influence 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 expanded three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our enterprise integrate cryptographic ancient such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics. We analysed the security of our schemes and quantified their computational and communication overhead.

ACKNOWLEDGMENT

This article has been written with the financial support of RUSA-Phase 2.0 grand sanctioned vide Letter No.F.24-51/2014-U. Policy (TNMulti-Gen).Dept. of Edn. Govt. of india, Dt.o9.10.2018

REFERENCES

[1] R. Ananadha Jothi V. Palanisamy, "Trust Based Association Estimation Technique on AODV Protocol Against Packet Droppers in MANET", International Journal of Applied Engineering Research,10 (55) (2015) 2408-2413.

[2] R. Ananadha Jothi and V. Palanisamy Various Attacks and Its Countermeasures in Mobile Ad Hoc Networks: A Survey International Journal of Engineering Research & Technology,3 (3) (2014) 50-57.

[3] J. Nithyapriya, R. Ananadha Jothi, V. Palanisamy, "Securing data with selective encryption based DAC scheme for MANET" , Computer Networks, Big Data and IoT. (Springer) Dec- 2018 (Accepted)

[4] J.NithyaPriya ,R.Anandha Jothi, V.Palanisamy, "Security scheme for MANET based on echoing and path changing"International Journal of Innovative science and research technology. 3 (10) (2018) 601-603.

[5] M. Jeevamaheswari, R. Anandha Jothi, V. Palanisamy ," AODV Routing Protocol to Defence Against Packet Dropping Gray Hole Attack In MANET", International Journal of Scientific Research in Science and Technology, 2018 IJSRST | Volume 4 | Issue 2 | Print ISSN: 2395-6011 | Online ISSN: 2395-602X.

[6] V. Anantharam and S. Verdu, "Bits through queues," IEEE Trans. Inf. Theory, vol. 42, no. 1, pp. 4–18, Jan. 1996.

[7] G. Morabito, "Exploiting the timing channel to increase energy efficiency in wireless networks," IEEE J. Sel. Areas Commun., vol. 29, no. 8,pp. 1711–1720, Sep. 2011.

[8] L. Galluccio, G. Morabito, and S. Palazzo, "TC-Aloha: A novel access scheme for wireless networks with transmit-only nodes," IEEE Trans.Wireless Commun., vol. 12, no. 8, pp. 3696–3709, Aug. 2013.

[9] W. Xu, W. Trappe, and Y. Zhang, "Anti-jamming timing channels for wireless networks," inProc. 1st ACM Conf. Wireless Netw. Security, 2008,pp. 203–213.

[10] S. D'Oro, L. Galluccio, G. Morabito, and S. Palazzo, "Efficiency analysis of jamming-based countermeasures against malicious timing channel in tactical communications," inProc. IEEE ICC, 2013, pp. 4020–4024.

[11] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies,"IEEE Netw., vol. 20, no. 3, pp. 41–47, May/Jun. 2006.

[12] R. Saranyadevi, M. Shobana, and D. Prabakar, "A survey on preventing jamming attacks in wireless communication," Int. J. Comput. Appl., vol. 57, no. 23, pp. 1–3, Nov. 2012.

[13] R. Poisel, Modern Communications Jamming Principles and Techniques. Norwood, MA, USA: Artech House, 2004, ser. Artech House information warfare library. [Online]. Available: http://books.google.it/books? Id=CZDXton6vaQC.

[14] R.-T. Chinta, T. F. Wong, and J. M. Shea, "Energy-efficient jamming attacks in IEEE 802.11 MAC," inProc. IEEE MILCOM, 2009, pp. 1–7.

[15] Y. W. Law, L. Van Hoesel, J. Doumen, P. Hartel, and P. Havinga, "Energyefficient link-layer jamming attacks against wireless sensor network MAC protocols," inProc. 3rd ACM Workshop Security Ad Hoc Sensor Netw. 2005, pp. 76–88.
[16] S. M. Bamakan, H.Wang, T.Yingjie, Y. shi, An effective instrusion detection framework based on MCLP/SVM optimized by timevarying chaos particle swarm optimization, Neurocomputing, Volume 199, 2016, page 90- 102.
[17] I. Yaqoob, E. Ahmed, M. H. Rehman, A. I. A. Ahmed, M. A. AlGaradi, M. Imran, M. Guizani, The rise of ransomware and emerging security challenges and solutions in the Internet of Things, Computer Networks, Vol. 129, Part 2, pp. 444-458, Dec, 2017.
[18] H. Wang, J. Gu, S. Wang, An effective intrusion detection framework based on SVM with feature augmentation, Knowledge-Based Systems, Volume 136, 2017, Pages 130-139, ISSN 0950-7051, https://doi.org/10.1016/j.knosys.2017.09.014.
[19] D. Gong, Y. Yang, and Z. Pan, "Energy-efficient clustering in lossy wireless sensor networks,"J. Parallel Distrib. Comput. vol. 73, no. 9, pp. 1323–1336, Sep. 2013.
[20] M. Ma, Y. Yang, and M. Zhao, "Tour planning for mobile data gathering mechanisms in wireless sensor networks, "IEEE Trans. Veh. Technol., vol. 62, no. 4, pp. 1472–1483, May 2013.
[21] M. Zhao and Y. Yang, "Bounded relay hop mobile data gathering in wireless sensor networks," IEEE Trans. Comput., vol. 61, no. 2, pp. 265–271, Feb. 2012.
[22] K. Xu, H. Hassanein, G. Takahara, and Q. Wang, "Relay node deployment strategies in heterogeneous wireless sensor networks,"IEEE Trans. Mobile Comput., vol. 9, no. 2, pp. 145–159, Feb. 2010.
[23] E. Lee, S. Park, F. Yu, and S.-H. Kim, "Data gathering mechanism with local sink in geographic routing for wireless sensor networks,"IEEE Trans. Consum. Electron. vol. 56, no. 3, pp. 1433–1441, Aug. 2010.
[24] B. Yang, J. Liu, S. Shenker, J. Li, and K. Zheng, "Keep forwarding: Towards K-link failure resilient routing," inProc. IEEE INFOCOM, Apr./May 2014, pp. 1617–1625.
[25] T. Elhourani, A. Gopalan, and S. Ramasubramanian, "IP fast reroutingfor multi-link failures," in Proc. IEEE INFOCOM, Apr./May 2014, pp. 2148–2156.
[26] T. Elhourani, A. Gopalan, and S. Ramasubramanian, "IP fast rerouting for multi-link failures," IEEE/ACM Trans. Netw., vol. 24, no. 5, pp. 3014–3025, Oct. 2016.
[27] M. Chiesa et al., "On the resiliency of static forwarding tables,"IEEE/ACM Trans. Netw., vol. 25, no. 2, pp. 1133–1146, Apr. 2016.
[28] S. Kini, S. Ramasubramanian, A. Kvalbein, and A. F. Hansen, "Fast recovery from dual-link or single-node failures in IP networks using tunneling," IEEE/ACM Trans. Netw., vol. 18, no. 6, pp. 1988–1999, Dec. 2010.
[29] W. Xu, K. Ma, W. Trappe, and Y. Zhang, "Jamming sensor networks: Attack and defense strategies,"IEEE Netw., vol. 20, no. 3, pp. 41–47, May/Jun. 2006.
[30] R.-T. Chinta, T. F. Wong, and J. M. Shea, "Energy-efficient jamming attacks in IEEE 802.11 MAC," inProc. IEEE MILCOM, 2009, pp. 1–7.
[31] D.G.Harkut, M.S.Ali and P.B.Lohiya, "Scheduling Task of Wireless Sensor Network Using Earliest Deadline First Algorithm" in ISROSET-Journal(IJSRCSE), vol.2, Issue.2, pp.1-6, Mar-2014.
[32] Umesh Kumar Singh, Jalaj Patidar and Kailash Chandra Phuleriya, "On Mechanism to Prevent Cooperative Black Hole Attack in Mobile Ad Hoc Networks" Isroset-Journal(IJSRCSE), vol.3, Issue.1, PP.11-15, Jan-2015.
[33] U.Korupolu, S.Kartik, and GK.Chakravarthi, "An Efficient Approach for Secure Data Aggregation Method in Wireless Sensor Networks With the Impact of Collusion Attacks" Isroset-Journal(IJSRCSE), vol.3, Issue.3, PP.26-29, Jan-2016.
[34] Lubdha M. Bendale, Roshani.L. Jain, Gayatri D.Patil, "Study of Various Routing Protocols in Mobile Ad-Hoc Networks"(IJSRNSC) Vol.06, Special Issue.01, PP.1-5, Jan-2018.
[35] Poonam Ahuja, "Bluetooth and Ad Hoc Networking" (IJSRNSC) Vol.1, Issue.2, PP.31-34, May-2013.

Authors Profile

Ms. T.Aruna is a currently pursuing M.Phil degree in Network Security at Department of Computer Applications in Alagappa University, Karaikudi, Tamil Nadu, India. She was completed B.sc(INFO TECH) and also complited M.C.A., degree. She do projects in biometrics, networks and security. Her main research involved in thrust areas such as Network Security and Ad-Hoc Networking. She has attended some international Conferences.Corresponding Author:

E-Mail: aruna1995mca@gmail.com

Mrs. R. Anandha Jothi is a DST-PURSE project fellow and currently project fellow in Rashtriya Uchchatar Shiksha Abhiyan (RUSA)-PHASE 2.0. Now she is pursuing Ph.D. degree and in Biometrics at Department of Computer Applications at Alagappa University, Karaikudi, Tamil Nadu, India. She was completed M.C.A., and M.Phil. degree. Her main research involved in thrust areas such as Network Security, Image Processing, Pattern Recognition and Ad-Hoc Networking. She has published more than 30 international journals and she has attended more than 15 international conferences.
E-Mail: ranandhajothi12@gmail.com

[1] Dr.PalanisamyVellaiyan obtained his B.Sc degree in Mathematics from Bharathidasan University in 1987. He also received M.C.A. and Ph.D. Degree from Alagappa University in 1990 and 2005 respectively. After working as Lecturer in AVVM Sri Pushpam College, Poondi Thanjavur from 1990 to 1995, He joined Alagappa University as Lecturer in 1995. He is currently working as Professor and Head of the Department of Computer Applications and Dean Student Affairsof the Alagappa University. He also received M.Tech. Degree from Bharathidasan University in 2009. He has published more than 120 international journals and he has attended 20 national conferences and 50 international conferences and his research interest includes Computer Networks & Security, Data Mining & Warehousing, Mobile Communications, Computer Algorithms and biometrics. Email: vpazhanisamy@yahoo.co.in

