International Journal on Recent and Innovation Trends in Computing and Communication ISSN 2321 – 8169
Volume: 1 Issue: 8 641 – 644

A New Approach for Jamming Attacks using -Packet-Hiding Methods

G.JAGADEESH KUMAR [1], B.PURUSHOTHAM [2]
[1] *M.Tech Pursuing, C.R. Engineering College, Tirupati.*
[2] *Asso.Professor, C.R. Engineering College, Tirupati.*

Abstract

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

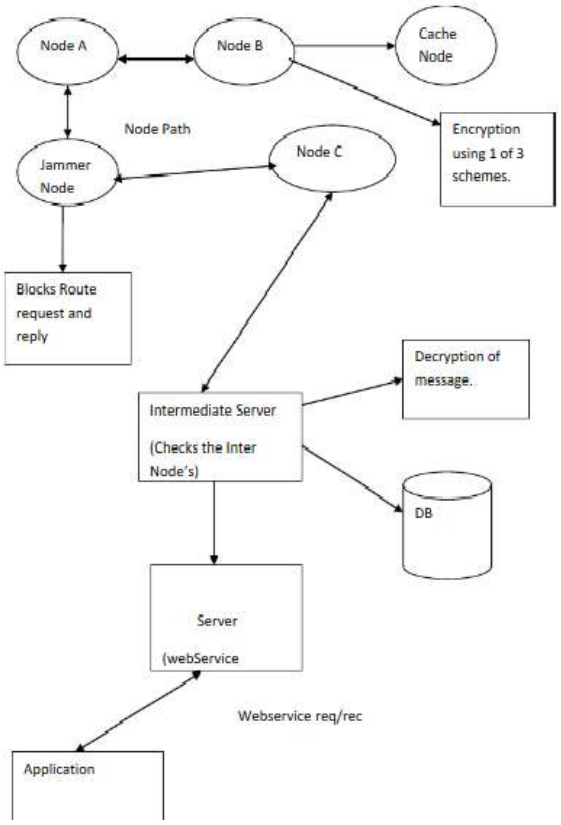
In this work, we address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing.

We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes. Our methods and evaluate their computational and communication overhead.

*

INTRODUCTION

To address the problem of jamming under an internal threat model and consider asophisticated adversary who is aware of network secrets and the implementationdetails of network protocols at any layer in the network stack. The adversaryexploits his internal knowledge for launching selective jamming attacks in whichspecific messages of high importance are targeted. For example, a jammer cantarget route-request/route-reply messages at the routing layer to prevent routediscovery, or target TCP acknowledgments in a TCP session to severely degradethe throughput of an end-to-end flow.The jammer may decode the first few bits of a packet for recovering useful packetidentifiers such as packet type, source and destination address. After classification,the adversary must induce a sufficient number of bit errors so that the packetcannot be recovered at the receiver.



EXISTING SYSTEM:

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 bitsaccording to a secret pseudo-noise (PN) code, known only to the communicatingparties. These methods can only protect wireless transmissions under the externalthreat model.

DISADVANTAGES OF EXISITNG SYTEM:

1. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions.
2. The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming.
3. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones.
4. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

PROPOSED SYSTEM:

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.

ADVANTAGES OF PROPOSED SYSTEM:

1. Relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes
2. Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer.
3. Achieve strong security properties

MODULES DESCRIPTION:

Real Time Packet Classification:

At the Physical layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m. Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node J. When A transmits a packet m to B, node J classifies mby receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B.

A Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Assume that the sender has a packet for Receiver. First, S constructs commit(message) the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is a randomly selected key of some desired key length s (the length of k is a security parameter).Upon reception of d, any receiver R computes.

Cryptographic Puzzle Hiding Scheme

A sender S has a packet m for transmission. The sender selects a random key k , of a desired length. S generates a puzzle (key, time), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second. After generating the puzzle P, the sender

broadcasts (C, P). At the receiver side, any receiver R solves the received puzzle to recover key and then computes.

Hiding based on All-Or-Nothing Transformations

The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet m is partitioned to a set of x input blocks m={m1,m2,m3 ….}, which serve as an input to an The set of pseudo -messages

m = {m1, m2, m3,…..} is transmitted over the wireless medium.

Service Categorization

The semantic categorization of UDDI wherein we combine ontologies with anestablished hierarchical clustering methodology, following the service descriptionvector building process. For each term in the service description vector, acorresponding concept is located in the relevant ontology. If there is a match, theconcept is added to the description vector. Additional concepts are added andirrelevant terms are deleted based on semantic relationships between the concepts.The resulting set of service descriptions is clustered based on the relationshipbetween the ontology concepts and service description terms. Finally, the relevantsemantic information is added to the UDDI for effective service categorization.

CONCLUSION:

An internal adversary model in which the jammer is part of the network underattack, thus being aware of the protocol specifications and shared network secrets. We showed that the jammer can classify transmitted packets in real time bydecoding the first few symbols of an ongoing transmission. We evaluated theimpact of selective jamming attacks on network protocols such as TCP androuting. Our findings show that a selective jammer can significantly impactperformance with very low effort. We developed three schemes that transform aselective 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 connection 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. *ACMTransactions 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.
[16] R. C. Merkle. Secure communications over insecure channels. *Com-
munications 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. ˇCapkun. Jamming-resistant broadcast communication without shared keys. In *Proceedings of the USENIX Security Symposium*, 2009.

About the Authors:

Mr. Jagadeesh kumar has pursing his M.Tech (CSE) Department at Chadalawada Ramanamma Engineering College. His areas interests datamining.

Mr. Purushotham working as Assoc.Professor of CSE Department at Chadalawada Ramananamma Engineering College, He has vast experience in Teaching field & Research.