International Journal of Science and Research (IJSR)
ISSN (Online): 2319-7064
Index Copernicus Value (2016): 79.57 | Impact Factor (2017): 7.296

A Detail Review of Jamming Attack Mitigation Techniques in Mobile Wireless Networks

Kalpana[1], Raj Kumar[2]

[1]M.Tech (CSE), RITM, Palwal, Maharshi Dayanand University, Rohtak, Haryana, India
Email: kalpana.geminian[at]gmail.com

[2]Department of CSE, RITM, Palwal, Maharshi Dayanand University, Rohtak, Haryana, India
Email: rajkumar23884[at]gmail.com

Abstract: ***From smart phones to wearable devices to Internet of Things (IoT)-based appliances, the demand for wireless communication keeps increasing. However, wireless communication consumes bandwidth, and the users inherently share a medium; therefore, one's signal becomes another's interference when they collide in channel access. To cope with the increased demand in wireless, the recent developments in radio technology facilitate flexible and dynamic access and enable better adaptation to the ongoing traffic for greater spectral efficiency. A survey of various techniques available for preventing jamming attacks in wireless networks have been presented in this paper. This paper also discusses three schemes to prevent selective jamming attacks in wireless networks. A selective jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission and can jam important messages. Three schemes that transform a selective jammer to a random one by preventing real-time packet classification are presented in this paper these schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristics. To mitigate these attacks, three schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes are also presented in this paper.***

Keywords: Selective jamming, denial-of-service, wireless networks, packet classification.

1. Introduction

Uninterrupted availability of the open wireless medium to interconnect the participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping 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 against wireless networks. Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Conventional antijamming 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 bits according to a secret pseudo noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. 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 cryptographic information. In this paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network 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. For example, a jammer can target route - request/route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics, or by decoding packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

2. Related Work

[1] Thuente and M. Acharya studied the impact of an external selective jammer who targets various control packets at the MAC layer in [6]. To perform packet classification, the adversary exploits interpacket timing information to infer eminent packet transmissions.

Y.W. Law et al. [7] have been proposed the estimation of the probability distribution of interpacket transmission times for different packet types based on network traffic analysis. Future transmissions at various layers were predicted using estimated timing information. Using their model, the authors proposed selective jamming strategies for well-known sensor network MAC protocols.

Liu et al. [8] have been proposed a smart jammer that takes into account protocol specifics to optimize its jamming

strategy. The adversary was assumed to target control messages at different layers of the network stack. 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.

3. Existing System

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods. Jamming attacks are much harder to counter. Typically, jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. In this model, jamming strategies include the continuous or random transmission of high-power interference signals. 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 bits according to a secret pseudo noise (PN) code known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model.

4. Literature Survey

In jamming Encrypted Wireless Ad Hoc Networks have been proposed by Timothy X Brown et al. [1]. This paper considered the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. Jamming is broken down into layers and this paper focuses on jamming at the Transport/Network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing.

Loukas Lazos et al. [2] have been proposed control-channel jamming attacks in multi-channel ad hoc networks. In deviating from the traditional view that sees jamming attacks as physical-layer vulnerability, to consider a sophisticated adversary who exploits knowledge of the protocol mechanics along with cryptographic quantities extracted from compromised nodes to maximize the impact of his attack on higher layer functions.

Wenyuan Xu et al. [3] have been proposed by four different jamming attack models that can be used by an adversary to disable the operation of a wireless network, and evaluate their effectiveness in terms of how each method affects the ability of a wireless node to send and receive packets, discuss different measurements that serve as the basis for detecting a jamming attack, and explore scenarios where each measurement by itself is not enough to reliably classify the presence of a jamming attack.

Timothy Wood et al. [4] have been proposed two strategies that may be employed by wireless devices to evade a MAC/PHY-layer jamming-style wireless denial of service attack. The first strategy, channel surfing, is a form of spectral evasion that involves legitimate wireless devices changing the channel that they are operating on. The second strategy, spatial retreats, is a form of spatial evasion whereby legitimate mobile devices move away from the locality of the DoS emitter. Paolo Codenotti et al. have been proposed an anti -jamming schedule for wireless data broadcast system in [5]. Modern society is heavily dependent on wireless networks for providing voice and data communications. Wireless data broadcast has recently emerged as an attractive way to disseminate dynamic data to a large number of clients. In data broadcast systems, the server proactively transmits the information on a downlink channel; the clients access the data by listening to the channel. Wireless data broadcast systems can serve a large number of heterogeneous clients, minimizing power consumption as well as protecting the privacy of the clients' locations, and also investigate efficient schedules for wireless data broadcast that perform well in the presence of a jammer.

The jamming attack is carried out in three different ways: constantly, randomly, and reactively. The implemented jammers are independent of the network protocols used in the WSN.

Constant Jamming: The constant jammer is the simplest attack model, in which the attacker uses the radio communication to constantly keep sending packet after packet. This results in the radio channel being blocked for all neighboring nodes. In our implementation on the TelosB motes, we directly access the physical layer transmitting method provided via the radio chip.

Random Jamming. Based on the constant jammer, the random jammer will choose random time intervals of jamming and non jamming. Hence, the regular nodes can successfully transfer messages from time to time, until the jamming blocks the communication again.

Reactive Jamming: A reactive jammer tries to cause a collision for every packet that it senses on the channel. For that purpose, it constantly listens to the channel and starts sending a predefined packet if it senses channel activity. If this is done fast enough, this single packet will cause a collision on the network layer. In order to realize this attack on actual sensor node hardware, the interrupt jamming attack as described in [17] was ported to Contiki.

We expect this attack to be hard to detect, since the jammer is only active for one packet each time. With no ongoing traffic, the attacker is silent. In addition, a successful collision also masks the jammer, because the channel is not readable at this moment. However, if the jammer fails to send its packet fast enough, its transmission can be observed.

Blackhole: A blackhole node tries to attract all the neighborhood traffic, but instead of forwarding, it discards all incoming data packets. Instead of forwarding this

traffic to the destination, it discards all incoming data packets. The implementations of this attack on the routing protocol need to be specifically adapted to mesh and collect networks. In the case of a mesh network, the blackhole node advertises route announcements with the best routing metric to all destinations. In a mesh network, the blackhole node advertises route announcements with the best routing metric to all destinations. It also replies to route requests by handling the incoming requests as the desired final destination and replying on behalf of it. CTP also requires some modifications for attracting the traffic. The blackhole node periodically broadcasts announcement messages with routing information which are used for selecting the parent node. In particular, it sets its own announcement routing metric to one in order to trick the other nodes into selecting it as parent. Since the base station has announcement value zero, a blackhole setting this value to zero would be suspicious. In addition, the blackhole will modify the routing information sent by other nodes, setting its costs again to one. Containing blackhole attacks is possible by using secure routing protocols [18], but preventing jamming attacks is difficult. Taking into account the characteristics of jamming and blackhole attacks in both collect and mesh networks, it is possible to develop specific detection approaches. However, we are interested in the actual impact of these attacks on real wireless sensor networks.

5. Proposed System

This paper aims to address the problem of jamming under an internal threat model, considering a sophisticated adversary who is aware of network secrets and the implementation details of network 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. To launch selective jamming attacks, the adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission. Such strategy can be actualized either by classifying transmitted packets using protocol semantics or by decoding packets on the fly. In the latter method, the jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. After classification, the adversary must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

A. Real Time Packet Classification

At the physical layer a packet is encoded, interleaved and modulated before it is transmitted over the wireless channel. At the receiver the packet needed to be decoded, deinterleaved and demodulated to recover the original packet.

B. Selective Jamming Module

To described the impact of selective jamming attacks on the network performance. Implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi -hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process 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. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher-text block.

C. Strong Hiding Commitment Scheme

SHCS is based on symmetric cryptography. Sender constructs commit message and transforms along with original information. A key is randomly selected; the length of key is a security parameter. Upon reception of message, any receiver computes using the key. In the SHCS message is modulated in the last few bits. To recover message any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of message.

D. Cryptographic Puzzle Hiding Scheme

The main idea of puzzle hiding is to make the receiver to solve the puzzle with predefined set of computation before the receiver gets the encrypted message. The receiver can solve the puzzle only when he receives full encrypted message.

E. Hiding Based On All-Or-Nothing Transformations

The packets are pre-processed by an AONT before transmission but remain encrypted. Here the original information is combined with the mapping message and a sequence of pseudo messages is generated. The Jammer cannot perform packet classification until all pseudo-messages corresponding to the original packets have been received and the inverse transformation has been applied. When a plaintext is pre-processed by an AONT before encryption, all cipher text blocks must be received to obtain any part of the plaintext.

6. Proposed System Design

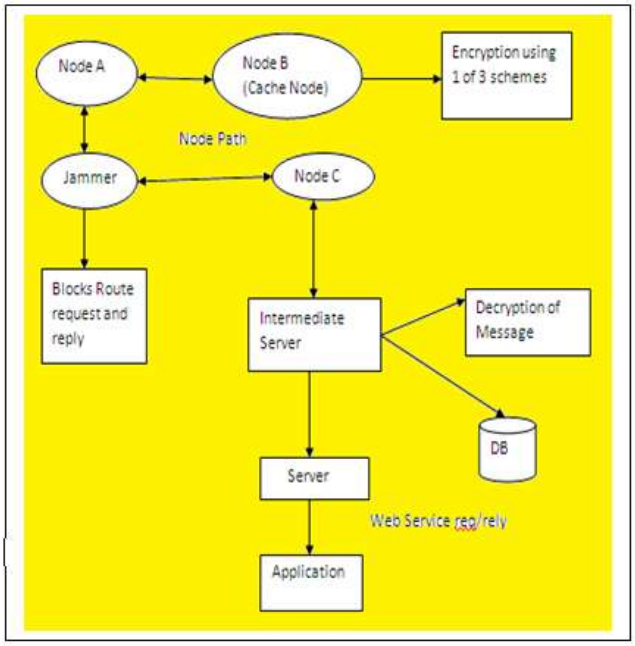

Figure 6.1: Proposed Architecture Design

Figure 6.1 shows the architecture diagram of the proposed system. The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within the communication range or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. For encrypted Communications, symmetric keys are shared among all intended receivers. These keys are established using preshared pairwise keys or asymmetric cryptography. 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. This is because for computationally efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packet to classify it.

7. Conclusion

A survey of various techniques available for preventing jamming attacks in wireless networks have been presented in this paper. This paper also discusses three schemes to prevent selective jamming attacks in wireless networks. A selective jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission and can jam important messages. Three schemes that transform a selective jammer to a random one by preventing real-time packet classification are presented in this paper these schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical-layer characteristic.

References

[1] T Brown, J.E James and A. Sethi 'Jamming and Sensing of Encrypted Wireless Ad Hoc Networks, ' Proceedings A International Symposium Mobile Ad Hoc Networking and Computing (MobiHoc) pp.120-130, 2006.
[2] L.Lazos S.iu and.Krunz ' Mitigating control- Channel Jamming Attacks in Multi- Channel Ad Hoc Networks, ' Proceedings Second ACM Conference Wireless Network Security, pp 169-180, 2009.
[3] W.Xu, W. Trappe, Y.Zhang, and T. Wood, 'The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks.' Proceedings ACM International Symposium Mobile Ad Hoc Networking and Computing (MobiHoc), pp-46-57, 2005.
[4] W.Xu, W.Tappe, and Y. Zhang. 'Channel Surfing and Spatial Retreats: Defense against Wreless Denial of Service, ' Proceedings Third ACM Workshop Wireless Security, pp. 80-89, 2004.
[5] Y.Desmett, 'Broadcast Anti-Jamming Systems, ' Computer Networks, vol.35, noc 2/3, pp. 223-236, Feb. 2001.
[6] D.Thuente, M. Acharya, 'Intelligent Jamming in Wireless Networks with Applications to 802.11b and other Networks, 'Proceedings IEEE Military Communication Conference (MILCOM), 2006.
[7] 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 Trans, Sensor Networks, Vol.5, no. 1, pp.1-38, 2009.
[8] X.Liu, G.Noubir and R. Sundaram, 'Spread : Foiling Smart Jammers Using Multi- Layer Agility, ' Proc. IEEE INFOCOM, pp 2536-2540, 2007.
[9] I. Krontiris, Z. Benenson, T. Giannetsos, F. C. Freiling, and T. Dimitriou, "Cooperative intrusion detection in wireless sensor networks, " in EWSN, 2009.
[10] F. Liu, X. Cheng, and D. Chen, "Insider attacker detection in wireless sensor networks, " in INFOCOM, 2007.
[11] T. Dimitriou and A. Giannetsos, "Wormholes no more? localized worm-hole detection and prevention in wireless networks, " in DCOSS, 2010.
[12] O. Gnawali, R. Fonseca, K. Jamieson, D. Moss, and P. Levis, "Collection tree protocol, " in SenSys, 2009.
[13] Y. Liu, Y. He, M. Li, J. Wang, K. Liu, L. Mo, W. Dong, Z. Yang, Xi, J. Zhao, and X.-Y. Li, "Does wireless sensor network scale? A measurement study on greenorbs, " in INFOCOM, 2011.
[14] M. Ceriotti, M. Corra, L. D'Orazio, R. Doriguzzi, D. Facchin, S. Guna, Jesi, R. Lo Cigno, L. Mottola, A. Murphy, M. Pescalli, G. Picco, Pregnolato, and C. Torghele, "Is there light at the ends of the tunnel? Wireless sensor networks for adaptive lighting in road tunnels, " in IPSN, 2011.
[15] J.-P. Vasseur and A. Dunkels, Interconnecting Smart Objects with IP: The Next Internet. Morgan Kaufmann, 2010.
[16] T. Winter, P. Thubert, and the ROLL Team, RPL: IPv6 Routing Protocol for Low-Power and Lossy Networks, http://www.rfc-editor.org/info/rfc6550,

RFC 6550 Std. [Online]. Available: http://www.rfc-editor.org/info/rfc6550
[17] A. D. Wood, J. A. Stankovic, and G. Zhou, "Deejam: Defeating energy-efficient jamming in ieee 802.15. 4-based wireless networks," in SECON, 2007.
[18] A. D. Wood, L. Fang, J. A. Stankovic, and T. He, "Sigf: A family of configurable, secure routing protocols for wireless sensor networks, " in SASN, 2006.
[19] R. Sen, A. Maurya, B. Raman, R. Mehta, R. Kalyanaraman, N. Vankad-hara, S. Roy, and P. Sharma, "Kyun queue: A sensor network system to monitor road traffic queues, ' SenSys 2012.
[20] H. Akaike, "Information theory and an extension of the maximum likelihood principle, " in Proceedings of the 2nd International Symposium on Information Theory, 1972.
[21] L. Sachs and J. Hedderich, Angewandte Statistik. Springer Berlin / Heidelberg, 2006.
[22] J. J. Louviere, D. A. Hensher, and J. D. Swait, Stated Choice Methods: Analysis and Applications. Cambridge University Press, 2000.
[23] S. Menard, Applied logistic regression analysis. Sage, 2002