Preventing Jamming Attacks in Wireless Sensor Networks Through Cryptography

[1]Nimmagadda.Hemanth Kumar, [2]Dr. P. Bala Krishna Prasad, [3]G. Guru Kesava Dasu
[1,2]Dept. of CSE, Eluru College of Engineeering and Technology, Eluru, WG, AP, India

Abstract
Understanding and defending against jamming attacks has long been a problem of interest in wireless communication and radar systems. In wireless ad hoc and sensor networks using multi-hop communication, the effects of jamming at the physical layer resonate into the higher layer protocols, for example by increasing collisions and contention at the MAC layer, interfering with route discovery at the network layer, increasing latency and impacting rate control at the transport layer, and halting or freezing at the application layer. Adversaries that are aware of higher-layer functionality can leverage any available information to improve the impact or reduce the resource requirement for attack success. For example, jammers can synchronize their attacks with MAC protocol steps, focus attacks in specific geographic locations, or target packets from specific applications. 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. We analyse the security of our methods By Adding Public Key Encryption algorithms (e.g., RSA) and evaluate their computational and communication overhead.

Keywords
MAC protocol, Selective Jamming RSA

I. Introduction

Computer users looking for convenience and mobility switch to satellite Internet. This includes going wireless which allows business travelers to use wireless blackberries to check their emails, vacationers to upload snapshots on their wireless laptops to show friends at home, consumers to make online payments from the comfort of their bed, and much more.
A wireless network can link up computers in different parts of your home, without a the need of a cord or a physical medium. Although, accessing the Internet wireless, proves convenient it also has its downside of being susceptible to hackers, particularly if you don't take the steps to secure your wireless network. So, learn some easy and quick steps to secure your network and about information systems security.

A. Types of Wireless Network Attacks: Jamming

Since RF (Radio Frequency) is essentially an open medium, jamming can be a huge problem for wireless networks. Jamming is one of many exploits used compromise the wireless environment. It works by denying service to authorized users as legitimate traffic is jammed by the overwhelming frequencies of illegitimate traffic. A knowledgeable attacker with the right tools can easily jam the 2.4 GHz frequency in a way that drops the signal to a level where the wireless network can no longer function.
The complexity of jamming is the fact that it may not be caused intentionally, as other forms of wireless technology are relying on the 2.4 GHz frequency as well. Some widely used consumer products include cordless phones, Bluetooth-enabled devices and baby monitors, all capable of disrupting the signal of a wireless network and faltering traffic.

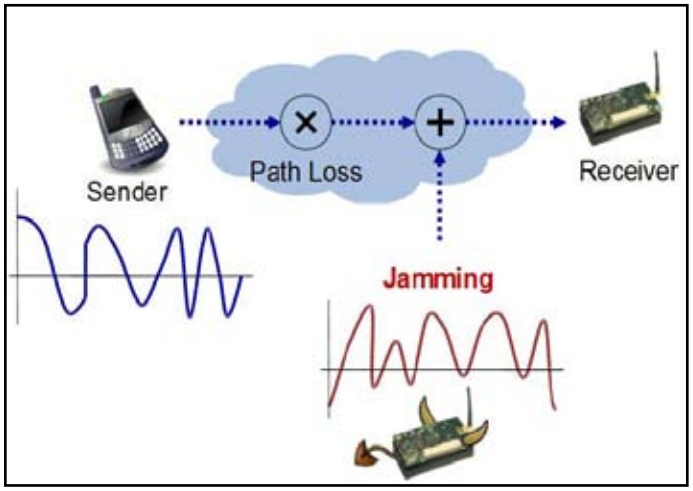


Fig. 1: Jamming Process

The issue of jamming mostly relates to older wireless local area networks as they are not fully equipped to make the adaptation to numerous types of interference. These networks typically call for an administrator to manually adjust each access point through trial and error. To avoid this daunting task, the best practice is to invest into a newer WLAN system. These environments offer real-time RF management features capable of identifying and adapting to unintentional interference.

B. Jamming Solutions

If an attacker truly wanted to compromise your LAN and wireless security, the most effective approach would be to send random unauthenticated packets to every wireless station in the network. This exploit can be easily achieved by purchasing hardware off the shelf from an electronics retailer and downloading free software from the internet. In some cases, it is simply impossible to defend against jamming as an experienced attacker may have the ability to flood all available network frequencies.
If the major concern relates to malicious jamming, an intrusion prevention and detection system may be your best option. At the bare minimum, this type of system should be able to detect the presence of an RPA (Rogue Access Point) or any authorized client device in your wireless network. More advanced systems can prevent unauthorized clients from accessing the system, alter configurations to maintain network performance in the presence of an attack, blacklist certain threats and pinpoint the physical location of a rogue device to enable faster containment.
It doesn't what type of interference you're experiencing; the network must have the ability to detect it, react and quickly make adjustments.

C. Identify the Presence of the Jammer

To minimize the impact of an unintentional disruption, it is important the identify its presence. Jamming makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer. The increased noise floor results in a faltered noise-to-signal ratio, which will be indicated at the client. It may also be measurable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. From there the access points must be dynamically reconfigured to transmit channel in reaction to the disruption as identified by changes at the physical layer. For example, if the attack occurred on an RF corresponding to channel 1, the access point should switch to channel 6 or 11 in order to avoid the attack. However, selecting a different channel does not always eliminate the issue of interference. An experienced attacker will often use all available channels in the attack. When this happens, your only option may be to physically hunt down the attacker and confront them face to face. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

D. Jamming Attack in Communication

In this section, we describe how the adversary can classify packets in real time, before the packet transmission is completed. Once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the generic communication system depicted in fig. 1. At the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless channel. At the receiver, the signal is demodulated, deinterleaved, and decoded, to recover the original packet m.

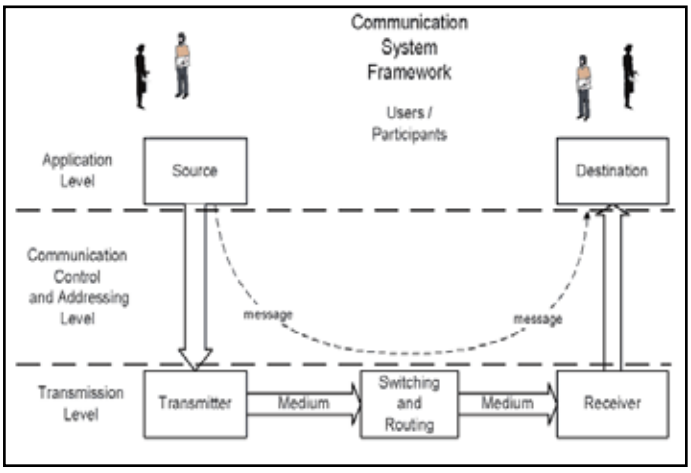


Fig. 2: Communication System

1. Impact of Selective Jamming

In this section, we illustrate the impact of selective jamming attacks on the network performance. We used OPNETTM Modeler 14.5 to 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.

2. Selective Jamming at the Transport Layer

In the first set of experiments, we setup a file transfer of a 3 MB file between two users A and B connected via a multi-hop route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/CTS mechanism was enabled. The transmission rate was set to 11 Mbps at each link. The jammer was placed within the proximity of one of the intermediate hops of the TCP connection. Four jamming strategies were considered:

- selective jamming of cumulative TCP-ACKs,
- selective jamming of RTS/CTS messages,
- selective jamming of data packets, and
- random jamming of any packet.

In each of the strategies, a fraction p of the targeted packets is jammed.

3. Implementation Details of SHCS

The proposed SHCS requires the joint consideration of the MAC and PHY layers. To reduce the overhead of SHCS, the decommitment value d (i.e., the decryption key k) is carried in the same packet as the committed value C. This saves the extra packet header needed for transmitting d individually. To achieve the strong hiding property, a sub layer called the "hiding sub layer" is inserted between the MAC and the PHY layer. This sub layer is responsible for formatting m before it is processed by the PHY layer. The functions of the hiding sub layer are outlined in fig. 2.

MAC header is 28 bytes long and has a total of 18 distinct fields. TCP header is 20 bytes long (assuming no optional fields) and has 17 distinct fields.

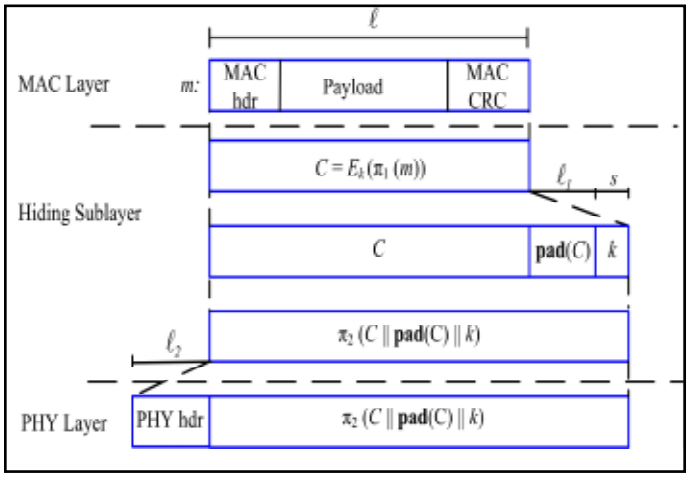


Fig. 3: Processing at the Hiding Sublayer

Assume the encryption of a fixed block of 128 bits. Packet $\pi 1(m)$ is partitioned to 146 plaintext blocks $\{p_1, p_2, \ldots, p_{146}\}$, and is encrypted to produce 146 ciphertext blocks $C = c_1||c_2|| \ldots ||c_{146}$. Each field of the TCP and MAC headers is distributed bit-by-bit from the Most Significant Bit (MSB) to the least significant bit (LSB) to each of the plaintext blocks in the reverse block order. This process is depicted in fig. 3.

The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thus\ avoiding the decryption operation at the receiver.

E. Cryptographic Puzzle Hiding Scheme (CPHS)

we present a packet hiding scheme based on cryptographic puzzles. The main idea behind such puzzles is to force the recipient of a puzzle execute a pre-defined set of computations before he is able to extract a secret of interest. The time required for obtaining the solution of a puzzle depends on its hardness and the computational ability of the solver. The advantage of the puzzle based scheme is that its security does not rely on the PHY layer parameters. However, it has higher computation and communication overhead

We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyse the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.

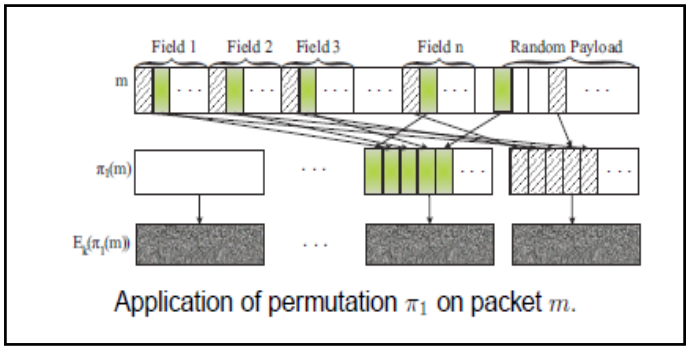


Fig. 4. Application of permutation π1 on packet m.

F. RSA Algorithm

A user of RSA creates and then publishes the product of two large prime numbers, along with an auxiliary value, as their public key. The prime factors must be kept secret. Anyone can use the public key to encrypt a message, but with currently published methods, if the public key is large enough, only someone with knowledge of the prime factors can feasibly decode the message. Whether breaking RSA encryption is as hard as factoring is an open question known as the RSA problem.

1. Operation

The RSA algorithm involves three steps: key generation, encryption and decryption.

2. Key Generation

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted in a reasonable amount of time using the private key. The keys for the RSA algorithm are generated the following way:

3. Choose Two Distinct Prime Numbers p and q.

For security purposes, the integers p and q should be chosen at random, and should be of similar bit-length. Prime integers can be efficiently found using a primality test.

(i). Compute n = pq.

n is used as the modulus for both the public and private keys. Its length, usually expressed in bits, is the key length.

(ii). Compute φ(n) = (p−1)(q−1), where φ is Euler's totient function.

(iii). Choose an integer e such that $1 < e < \varphi(n)$ and greatest common divisor $\gcd(e, \varphi(n)) = 1$; i.e., e and φ(n) are coprime.

- e is released as the public key exponent.
- e having a short bit-length and small Hamming weight results in more efficient encryption – most commonly $2^{16} + 1 = 65{,}537$. However, much smaller values of e (such as 3) have been shown to be less secure in some settings.

4. Determine d as $d \equiv e^{-1} \pmod{\varphi(n)}$, i.e., d is the multiplicative inverse of e (modulo φ(n)).

- This is more clearly stated as solve for d given $de \equiv 1 \pmod{\varphi(n)}$
- This is often computed using the extended Euclidean algorithm.
- d is kept as the private key exponent.

By construction, $d \cdot e \equiv 1 \pmod{\varphi(n)}$. The public key consists of the modulus n and the public (or encryption) exponent e. The private key consists of the modulus n and the private (or decryption) exponent d, which must be kept secret. p, q, and φ(n) must also be kept secret because they can be used to calculate d.

- An alternative, used by PKCS#1, is to choose d matching $de \equiv 1 \pmod{\lambda}$ with $\lambda = \text{lcm}(p-1, q-1)$, where lcm is the least common multiple. Using λ instead of φ(n) allows more choices for d. λ can also be defined using the Carmichael function, λ(n).
- The ANSI X9.31 standard prescribes, IEEE 1363 describes, and PKCS#1 allows, that p and q match additional requirements: being strong primes, and being different enough that Fermat factorization fails.

D. Encryption

Alice transmits her public key (n, e) to Bob and keeps the private key secret. Bob then wishes to send message M to Alice.

He first turns M into an integer m, such that $0 \leq m < n$ by using an agreed-upon reversible protocol known as a padding scheme. He then computes the ciphertext c corresponding to

$$c \equiv m^e \pmod{n}.$$

This can be done quickly using the method of exponentiation by squaring. Bob then transmits c to Alice.

E. Decryption

Alice can recover m from c by using her private key exponent d via computing

$$m \equiv c^d \pmod{n}.$$

Given m, she can recover the original message M by reversing the padding scheme.

By using RSA in Password Resistant Protocol give better security and protect the system in a consistent way

V. Conclusion

We addressed the problem of selective jamming attacks 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 ongoing transmission. We evaluated the impact 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 developed three schemes that transform a selective jammer to a random one by preventing real-time packet classification. Our schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer

characteristics. We analyzed the security of our schemes by adding RSA algorithm in transmission and quantified their computational and communication overhead.

In this paper, we addressed the problem of online dictionary attacks and presented an authentication protocol to counter the same. In the protocol, the client is required to compute the response to the presented challenge. Online password guessing attacks on password-only systems have been observed for decades. Computing this response is deliberately designed to be a time taking operation thus ensuring that the client is not able to launch a large number of login requests in a small amount of time. The protocol is designed in a fashion such that the computation of this response does not poses any problems for a legitimate user since she may reuse the last computation, but is time consuming and costly for an adversary trying to launch thousands of login requests per second.

Consider k2 = 3, p = 0:05, b1 = 5, and b2 = 5, for concreteness

In previous ATT-based login protocols, there exists a security usability trade-off with respect to the number of free failed login attempts (i.e., with no ATTs) versus user login convenience (e.g., less ATTs and other requirements). In contrast, PGRP is more restrictive against brute force and dictionary attacks while safely allowing a large number of free failed attempts for legitimate users. Our empirical experiments on two data sets (of one-year duration) gathered from operational network environments show that while PGRP is apparently more effective in preventing password guessing attacks (without answering ATT challenges), it also offers more convenient login experience, e.g., fewer ATT challenges for legitimate users even if no cookies are available. By encrypting the keys by using RSA the security become good. However, we reiterate that no user testing of PGRP has been conducted so far. PGRP appears suitable for organizations of both small and large number of user accounts.

References

[1] Alejandro Proano, Loukas Lazos,"Packet-Hiding Methods for Preventing Selective Jamming Attacks", IEEE Transactions On Dependable And Secure Computing ,Vol. 9, No. 1, Jan-Feb 2012.

[2] M. Cagalj, S. Capkun, J.-P. Hubaux,"Wormhole-based antijamming techniques in sensor networks", IEEE Transactions on Mobile Computing, 6(1), pp. 100–114, 2007.

[3] A. Chan, X. Liu, G. Noubir, B. Thapa,"Control channel jamming: Resilience and identification of traitors", In Proceedings of ISIT, 2007.

[4] T. Dempsey, G. Sahin, Y. Morton, C. Hopper,"Intelligent sensing and classification in Ad-Hoc networks: A case study", Aerospace and Electronic Systems Magazine, IEEE, 24(8), pp. 23–30, August 2009.

[5] Y. Desmedt,"Broadcast anti-jamming systems", Computer Networks, 35(2-3), pp. 223–236, February 2001.

[6] K. Gaj and P. Chodowiec,"FPGA, ASIC implementations of AES", Cryptographic Engineering, pp. 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, D. Wetherall,"Improving wireless privacy with an identifier-free link layer protocol", In Proceedings of MobiSys, 2008.

[9] IEEE.IEEE802.11standard, [Online] Available: http://stadards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.

[10] A. Juels, J. Brainard,"Client puzzles: A cryptographic countermeasure against connection depletion attacks", In Proceedings of NDSS, pp. 151–165, 1999.

[11] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, P. Havinga,"Energy-efficient link-layer jamming attacks against WSN MAC protocols. ACMTransactions on Sensors Networks, 5(1), pp. 1–38, 2009.

[12] L. Lazos, S. Liu, M. Krunz,"Mitigating control-channel jamming attacks in multi-channel Ad-Hoc networks", In Proceedings of the 2nd ACM conference on wireless network security, pp. 169–180, 2009.

[13] G. Lin, G. Noubir,"On link layer denial of service in data wireless LANs", Wireless Communications and Mobile Computing, 5(3), pp. 273–284, May 2004.

[14] X. Liu, G. Noubir, R. Sundaram,"Spread: Foiling smart jammers using multi-layer agility", In Proceedings of INFOCOM, pp. 2536– 2540, 2007.

[15] Y. Liu, P. Ning, H. Dai, 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), pp. 294–299, 1978.



Nimmagadda Hemanth Kumar received His B.tech Degree in computer Science From Sir C. R. Reddy College of Eng, Eluru,, in 2011, the M.TECH. degree in CSE from Eluru College of Engineering and Technology, Eluru in 2011-13. At present, He is engaged in "preventing jamming attacks in wireless sensor network through cryptography".



Dr. P. Bala Krishna Prasad is the Principal of Our Eluru College of Engineering & Technology, Eluru. He obtained Doctoral Degree in Engineering, Ph.D(CSE) from Acharya Nagarjuna University, in the year 2007. He received his Master's Degree I n Engineering, M.Tech (CSE) from Andhra University in the year 2000. He completed His Bachelor's Degree in Engineering, B.Tech (CSE) from IETE, New Delhi.He has a rich experience of 18 years which includes Teaching, Research and Administration. He served various reputed engineering colleges as a Principal for several years. He is a multi-tasking personality and ago getter. His relentless efforts and commitment in Institutional Administration lead few colleges to reach greater heights.He published several technical papers in National and International Journals of repute. He is a most coveted author for Computer Science and Information Technology subjects and has 7reputed text books in his authorship. Under his able guidance several research scholars are pursuing their Doctoral and Pre Doctoral Programs in various Universities



Prof. G.Guru Kesava Dasu received M. Tech (I.T) Degree in 2003 and received M.E (C.S.E) Degree from ANNA University in 2008. He is having12 years of Teaching Experience in various Engineering Colleges. At present he is working as Professor & HOD, Department of CSE, Eluru College of Engineering & Technology, Eluru. He is a certified professional of IBM Rational Rose from Rational University.