ISSN No: 2348-4845
International Journal & Magazine of Engineering, Technology, Management and Research
A Peer Reviewed Open Access International Journal

A real-time Packet Classification Scheme Combined with Cryptography to Mitigate Jamming Attacks

Mavidi Chakravarti
M.Tech Student(Software Engineering) ,
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and
Mangement, Srikakulam, Andhra Pradesh.

B.Vineela
Assistant Professor
Department of Computer Science and Engineering,
Sarada Institute of Science Technology and
Mangement, Srikakulam, Andhra Pradesh.

Abstract:

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.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.Wireless Networks are becoming an increasingly important technology that is bringing the world closer together. In this type of network environment there could be more chances of attacks. The packets cannot be easily transferred over the network. It affects network performance degrade. 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 networks. In Simplest form adversary blocks the packets that are transmitted over wireless network. Typically, jamming attacks has been considered under an external threat model, in which the jammer is not part of the network. To overcome the above problem of network traffic and performance in this paper we have considered a packet hiding methods that can be securely transmit packets over the network.

We are addressing the problem of jamming attacks under internal threat model and two schemes are proposed that prevent real-time packet classification of packets by combining hiding scheme based on cryptographic primitives.

Keywords:

Jamming signals, Strong hiding commitment scheme, cryptographic puzzle hiding scheme, Wireless networks, denial-of-service.

Introduction:

Jamming is usually distinguished from interference that can occur due to device malfunctions or other accidental circumstances. Devices that simply cause interference are regulated under different regulations. Unintentional 'jamming' occurs when an operator transmits on a busy frequency without first checking whether it is in use, or without being able to hear stations using the frequency. Another form of unintentional jamming occurs when equipment accidentally radiates a signal, such as a cable television plant that accidentally emits on an aircraft emergency frequency.

Originally the terms were used interchangeably but nowadays most radio users use the term "jamming" to describe the deliberate use of radio noise or signals in an attempt to disrupt communications (or prevent listening to broadcasts) whereas the term "interference" is used to describe unintentional forms of disruption (which are far more common). However the distinction is still not universally applied. For inadvertent disruptions, see electromagnetic compatibility.

Intentional communications jamming is usually aimed at radio signals to disrupt control of a battle. A transmitter, tuned to the same frequency as the opponents' receiving equipment and with the same type of modulation, can, with enough power, override any signal at the receiver. Digital wireless jamming for signals such as Bluetooth and WiFi is possible with very low power.

The most common types of this form of signal jamming are random noise, random pulse, stepped tones, warbler, random keyed modulated CW, tone, rotary, pulse, spark, recorded sounds, gulls, and sweep-through. These can be divided into two groups – obvious and subtle.Obvious jamming is easy to detect because it can be heard on the receiving equipment. It usually is some type of noise such as stepped tones (bagpipes), random-keyed code, pulses, music (often distorted), erratically warbling tones, highly distorted speech, random noise (hiss) and recorded sounds. Various combinations of these methods may be used often accompanied by regular morse identification signal to enable individual transmitters to be identified in order to assess their effectiveness. For example, China, which used jamming extensively and still does, plays a loop of traditional Chinese music while it is jamming channels (c.f. Attempted jamming of number stations).

The purpose of this type of jamming is to block reception of transmitted signals and to cause a nuisance to the receiving operator. One early Soviet attempt at jamming western broadcasters used the noise from the diesel generator that was powering the jamming transmitter.Subtle jamming is jamming during which no sound is heard on the receiving equipment. The radio does not receive incoming signals yet everything seems superficially normal to the operator. These are often technical attacks on modern equipment, such as "squelch capture". Thanks to the FM capture effect, frequency modulated broadcasts may be jammed, unnoticed, by a simple unmodulated carrier. The receiver locks onto the larger carrier signal and hence will ignore the FM signal with information.

Digital signals use complex modulation techniques such as QPSK. These signals are very robust in the presence of interfering signals. However, the signal relies on hand shaking between the transmitter and receiver to identify and determine security settings and method of high level transmission.

If the jamming device sends initiation data packets the receiver will begin its state machine to establish two way data transmission. A jammer will loop back to the beginning instead of completing the handshake. This method jams the receiver in an infinite loop where it keeps trying to initiate a connection but never completes it, which effectively blocks all legitimate communication.Bluetooth and other consumer radio protocols such as WiFi have built in detectors so that they only transmit when the channel is free. Simple continuous transmission on a given channel will continuously stop a transmitter transmitting, hence jamming the receiver from ever hearing from its intended transmitter. Other jammers work by analysing the packet headers and depending on the source or destination, selectively transmit over the end of the message, corrupting the packet.

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.

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.

Wireless networks are computer networks that are not connected by cables of any kind. Wireless System enables wireless connectivity to the Internet via radio waves rather than wires on a personals home computer, smartphone, laptops or similar mobile device. The use of a wireless network makes enterprises to avoid the costly process of introducing cables into buildings or as a connection between different equipment locations. The bases for wireless systems are radio-waves; it means an implementation that takes place at the physical level of network structure.

In the computing world, the term wireless can be used as ambiguous, since it may refer to several different wireless technologies. Wireless Networks are becoming an increasingly important technology that is bringing the world closer together. Wireless Networks are used in every area, such as agriculture, education, pharmaceuticals, manufacturing, military, transportation and research. Therefore, the importance of Wireless Networks security is significant. Security is one of the critical attributes of any communication network. Various attacks were reported over the last many years.

Wireless networks are highly sensitive to Denial of Service (DoS) attack. A Denial of Service (DoS) attack can be characterized as an attack with the purpose of preventing legitimate users from using a specified network resource such as a website, web service, or computer system.The wireless communication medium is a broadcast channel, exposing physical layer of wireless communication to jamming.

Past research has mostly focused on defending voice communication using spread spectrum techniques. The SS techniques provide bitlevel protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties.

Such approach spreads the signal into a very large frequency band and makes a jammer with limited energy resources unable to afford jamming the entire band. These methods only protect wireless transmissions under the external threat model. Non-continuous jamming only results in a graceful degradation of the voice quality. Therefore, this approach is effective to protect voice communication against jamming.

Existing System:

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect 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. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or severalshort jamming pulses. Typically, jamming attacks have been considered underan external threat model, in which the jammer is not part of the network. To prevent the jamming attack we are propose the following technique.

Proposed System:

The proposed system is used to prevent selective jamming attack in wire less network. This can be overcome by using random padding signature algorithm for preventing jamming attacks. Before performing the random padding signature we are generating random number for generation of signature. The procedure of random padding signature algorithm has follows.

Radom padding signature Algorithm :

Step 1. A large prime number p is produced by system, α is a generator of Zp*, x(1<x <(p)) is the signer's private key, the corresponding signature public keyβ can be calculated byβ =α xmod p , and opened to the public key.

Step2 . Two different random number t and k are randomly selected by system. Where t, k and x must be coprime and there is inverse.γ and λ are calculated by the γ =α kmod p , λ =α tmod p and retainγ and λ .

Step3: Signature explicitly m, δ is calculated using the results of the first two steps as well as the extended Euclidean algorithm and modular inversion algorithm by m = (xγ + kλ + tδ)mod(p −1) . It should be avoided to take the same random number and simple functional relationship exists between random numbers at the course of obtaining a number of signatures.

Step4: Discarded the random number k and t, then the required public key p, β and α are obtained. The private key is x. The signature of plain text m is (γ ,λ ,δ) .
Encryption and Decryption process:

Before Transferring message the sender will encrypt message using QR technique for converting plain format to cipher format. The proposed technique uses any standard encryption technique which incorporates lossless compressionin order to cater to the needs of low bandwidth and data security. As mentioned above, let L be a defined language over the alphabet set _. For example, L be English and _ be {A,B, . . . Z,a, b, . . . , z}. Let the letters of _ be indexed by a bijection function I that maps a letter to an integer i, where 1 ≤ i ≤ |_|. Δ is a constant, called modulus constant. Let the data string M be {m1,m2,m3, . . . , mn} _. Performing modulus operation on every I(mi) by Δ, sequentially yields remainder set R as {r1, r2, r3, . . . , rn} and quotient set Q as {q1, q2, q3, . . . , qn}. The elements in R havie the values between [0,Δ− 1]. So, we consider the elements in R to be a vector of numbers in base R. Each ritakes _log2 R_ bitsfor binary representation. If the message is of n characters, the number of bits required to represent the vector R is n × _log2 R_. The quotient set is represented in a different way. Let B = _|_|Δ_+1 be another parameter called Base-valuer. The elements of Q will have values within [0,B−1]. Consider Q as a number in base B, i.e. (q1, q2, . . . ,qn)B. Convert the number to a higher base. It is obvious that a higher base representation would reduce the digits in the number. If B is less then10, the we convert QB to a Q10 number.

The Encoding Algorithm can be stated as :
1) Input: M
2) n= |M| , i.e. length of M
3) Z = n × bit size
i.e. bit size is the number of bits require to represent each charecter.
4) fori = 1 to n
4.1) Read mi the ithcharacter from M.
4.2) Find R
R[i] = I(mi)%Δ
4.3) Find Q
Q[i] = I(mi)/Δ
5) Representation of R
fori = 1 to n
5.1) Represent R[i] in Base Δ.
6) Representation of Q

Interpret Q as Base B number and convert it to Base 10
The vector R is communicated through open channel, whereas Q is encrypted to a cipher Qcusing any standard cryptographic technique and communicated to the receiver to ensure the confidentiality of the message M. By doing so, the overhead of encryption is reduced as we encrypt only tuple Q, rather than the whole message M. The receiver on receiving R and Qc, decrypts Qc to Q and decodes the message from the bituple
< R,Q>.

The Decoding Algorithm as follows:
1) Input: Bi-tuple < R,Q>
2) Convert Q from Base 10 to Base B
Let QB = (q1, q2, . . . ,qn) be the representation in Base B

3) Interpret R as a vector of Base Δ number

4) for1 ≤ i ≤ n

4.1) i = qi ×Δ+ri
whereqi the ithdigit of QB rithe ithelement of R.

4.2) mi = I−1(i)
5) M = (m1,m2, . . . , mn)

Verification :

Step5: (γ ,λ ,δ) is sent to the corresponding customers by system. The customers use the following equation to verify the correctness of plaintext m digital signatures. If equal, the signature is correct. Otherwise, the signature is incorrect or transmission errors. The equation as follows:
$\alpha m = \beta \gamma\gamma\lambda\lambda\delta$ mod p

They are equal then retrieve the packet . If not equal discard packets sended by sender to the verifier. This way we can preventing the selective jamming attack.

CONCLUSIONS:

The problem of selective jamming attacks under internal threat model is considered. Here jammer is part of the network under attack, thus being aware of the protocol specifications and shared network secrets. To avoid packet classification in wireless transmission we proposed two schemes such as commitment scheme based on strong hiding and hiding based on cryptographic puzzle. These two schemes prevent the jammer from blocking the packets that is transmitted over wireless network so that the data reaches the receiver without any inaccuracies.

REFERENCES:

[1] Alejandro Proan˜o and LoukasLazos,” Packet-Hiding Methods for Preventing Selective Jamming Attacks”, ieee transactions on dependable and secure computing, vol. 9, no. 1, january/february 2012.

[2] 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.

[3] 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.

[4] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001. Y. Desmedt. Broadcast anti-jamming systems. Computer Networks,35(2-3):223–236, February 2001.

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

[6] T. X. Brown, J. E. James, and A. Sethi. Jamming and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages120–130, 2006.

[7] 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.

[8] L. Lazos, S. Liu, and M. Krunz.Mitigating control-channel jamming attacks in multi-channel ad hoc networks. In Proceedings of the 2ndACM conference on wireless network security, pages 169–180, 2009.

BIOGRAPHIES:

Mavidi Chakravarti

student in M.Tech(CSE) in Sarada Institute of Science Technology and Management, Srikakulam. He has received his B.tech(IT) Thandra paparaya instituute of science and technology bobbili ,vizianagaram (dist). His interesting areas are data mining, computer network.

Behara Vineela

is working as Asst.professorin Sarada Institute of Science, TechnologyAnd Management, Srikakulam, AndhraPradesh. He received his M.Tech (CSE)from AITAM ,Tekkali, Srikakulam, Andhra Pradesh. JNTU Kakinada Andhra Pradesh.His research areas include Network Security