www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume 4 Issue 5 May 2015, Page No. 12033-12039

Wireless Networks – Analysis on Prevention of Jamming Attacks

Ramesh Kumar Mojjada
Mtech CSE MVGR College of engineering

Abstract –Jamming a wireless communication device that transmits on the same frequency range as a cell phone to create strong cell tower interference and block cell phone signals and call transmission. Jammers are usually undetectable and may experience minimal effects such as poor signal reception and devices may be used in any location but are typically deployed where cell phone use may be disruptive or wireless may get vulnerable to interference attacks. To prevent from jamming in any communication hiding the information is the best concern typically jamming has been addressed under an external threat model.Adversary is a short period of time, jammer selectivelytargeting messages of priority high importance. Our analysis providesprevention of jamming in terms of network performance degradation andeffort by presenting machine learning algorithm like clustering & Classification, a selective attack on wireless network on routing. We show comparative work on jamming attacks can belaunched by performing real-time packet classification. Cryptographic primitive is hides the data, to mitigate the attacks prevents real time packet classification, provides the security communication.

Keywords - Cryptography, Jamming Attacks, Wireless Networks, Authentication, Security.

INTRODUCTION I

Wireless networks rely on susceptible to numerous security threats due to the open nature of the wireless medium. Transceiver can eavesdrop on ongoing transmissions, inject spurious messages, or block the transmission of legitimate ones. One of the ways for degrading the network performance issue is by jamming wireless transmissions. Method of jamming, the adversary corrupts transmitted messages by causing electromagnetic interference in the network's operational frequencies, and in proximity to the targeted receivers. As these networks gain popularity, providing security and trustworthiness will become an issue of critical importance. Many wireless security threats may be addressed through appropriately designed network security architectures, which are essentially modifications of traditional security services, such as confidentiality, authentication, and integrity to the wireless domain. Wireless networks, however, are susceptible to threats that are not able to be adequately addressed via cryptographic methods. One serious class of such threats is attacks of radio interference. Nature of the shared wireless medium, combined with the commodity nature of wireless technologies and an increasingly sophisticated user-base, allows wireless networks to be easily monitored and broadcast on. Adversaries may easily observe communications between wireless devices, and just as easily launch simple denial of service attacks against wireless networks by injecting false messages. Wireless radio signals are uses in the scenario attacker may have a stronger antenna for signal generator first attacker identifies the signal patterns around the target Access Point then creates the same frequency pattern radio signals and start transmitting in the air in order to create a signal tornado of a wireless network. As a result target Access Point gets jammed on top of that the legitimate user node also gets jammed by signals

and disables the access point connection between legitimate user of wireless network and the network itself. Attacker may spoof the packers and send it to the victim in order to take control over user's machine or network.

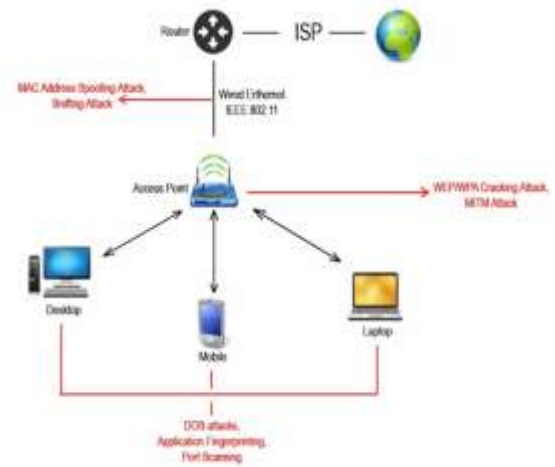

Figure 1 Represents the Jamming Attacks in Wireless Networks.

Attack takes place when fake or rough RF frequencies are making trouble of the legitimate wireless network operation other cases false positive such as cordless phone uses the identical frequency as the wireless network users but it is actually not a jamming of signal very common attack as it require a ton of capable hardware.

SECTION II

2. Related Work: Jamming attack can detect with effective energy efficient or protocol aware, some of metrics characterizing the protocol aware so that they are less likely to detect, authentication of users, strength against FEC codes and physical layer to beat channel coding techniques and energy conservation. Measures like PDR PSR CST are to detect jamming attack influenced by channel fading network congestion or link failure. Adaptive threshold like BMAC protocol is suggested but it has the drawback of continuously increasing the transmission power eventually jammer blasting at channel and detector which shows the channel idle.If an attacker wanted to compromise LAN and wireless security most effective approach would be to send random unauthenticated packets to wireless station in the network. Exploit can be easily achieved by purchasing hardware off the shelf from an electronics retailer and downloading free software from the internet. Major concern relates to malicious jamming an intrusion prevention and system detect may be your best option at minimum should be able to detect the presence of an Rogue Access Point of authorized client device in wireless network. To minimizethe impact of an unintentional disruption it is important to identify its presence jamming makes it know at the physical layer of the network commonly as Media Access Control which increase noise floor in a faltered noise to signal ratio which will be indicated at the client. Measureable from the access point where network management features should able to effectively report noise floor levels that exceed a predetermined threshold. For example if the attack occurred on an RF corresponding to channel1 the access point should switch to channel 6 or 11 in order to avoid the attack selecting a different channel does not always eliminate the issue of interference.

SECTION III

3. Attacks in Wireless Networks: Wireless network is eliminating the complex tidy cable which acquires space and not spoiling the look of working area in the network but we know that each coin has two sides. There are benefits and demerits of wireless networks as well comes with high possibility of attacks, in WLAN protocol IEEE 802.11 protocol commonly used for the wireless networking participants must have transmission and receivers to sending and receiving signals.

3.1. Injection Attack 802.11: An attacker must have a clear understanding of protocol any hacker will perform method in order to perform injection attack on wireless networks first will perform passive injection attack on wireless then attacker creates wireless protocol frames in order to send it to the targeted network we have two options one is create a false packet and insert it to that network other is sniff the network traffic once these packets are sent to server response from that wireless network is captured intercepted and modified by an attacker to perform man in the middle attack.

3.2. Denial of Sleep Attack: Sometimes wireless networks not use radio transmission to reduce the consumption it regulates the

communication of that particular node malicious user can take benefit of mechanism. Attacker may drain the power supply of the sensor device in order to make node life very short attacker attack on MAC layer to reduce the sleep period of it. If the number of drained node goes high whole network can be disrupted only MAC protocol has an ability to create longer sleep duration cannot extend the life time of wireless network.

3.3. Collision Attack: In this type of attack, attacker tries to spoil the packets to be transmitted at the receiver. So when attacker gets succeeded then the resulting packet's check sum will not be expected at receiver's end. As a result of that, whole packet will be discarded at receiver's node. Now retransmission of that packet will consume high energy of that particular sensor node. Second Approach of collision attack can be defined as this. Sometime message gets transmitted on the node via same frequency it can also generate collision.

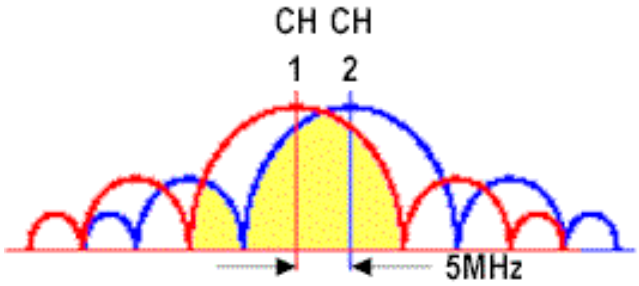

Figure 2 Collision Attack

Figure shows the yellow area is channel 2's signals are overlapping on to the channel one's work area. So the amount of channel 2's work area is overlapping in channel one's work area, both the channels will suffer the in communication.

3.4. De-Synchronization Attack: In this attack, attacker tries to modify the control flags and sometimes the sequence numbers in order to forge the packets, or messages. As a result, attacker limits the legitimate user from exchanging the messages between server and client. It will continuously request for retransmission of those messages. This attack causes infinite cycle of the retransmission. It acquires a lot of energy. We can also say that attacker disturbs the established connection between two end points.

3.5. Flooding Attack: Plenty of DoS attacks which reduces the network lifetime in different ways and manner. One of the common methods is denial of service attack. Attacker sends huge amount of packets in order to stop the networking from being communicating with different nodes. Main aim for this attack is exhaust the resources on the victim's machine.

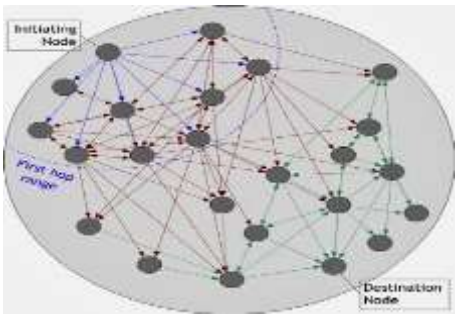

Figure 3 is a flooding Attack in Networks

3.6. Replay Attack: In this process data of the transmission is repeated maliciously. Attacker intercepts the data in order to retransmit it further. It's a part of masquerade attack which can be carried away by substitution of an IP packet. A stream cipher attack can be taken place into that.

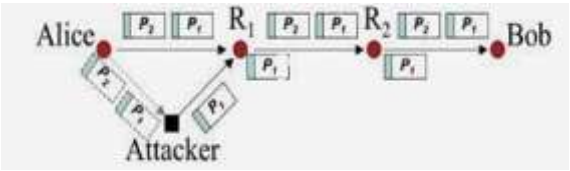

Figure 4 is a Replay Attack in Networks

Attacker repeats the copies of the packets to the victim in order to exhaust the energy or power supply. This kind of attack has ability to crash applications which are designed poorly.

3.7. Selective Forwarding Attack: It may also refer as 'gray hole attack'. In this form of attack, attacker may stop the node to pass packets through in by forwarding or dropping those messages. In form of selective forwarding attack, node selectively rejects the packets by dropping them coming into that network from an individual node or the group of individual nodes. Malicious node is selectively dropping packets from certain group of node, forward it to somewhere else which will create no trustable routing information due to forwarding packets to any wrong path within the network.

3.8. Unauthorized Routing Update Attack: In routing process many components take place such as hosts, base station, access points, nodes, routing protocols etc.. Malicious user may try to update all these information in order to update the routing table. It may possible that due to this attack, some of the nodes get isolated from the base station. Also network partition may occur due to this attack. Packets may drop after TTL gets expired. Packets can be forwarded to any unauthorized user. All these incidents are the impact of this attack.

3.9. Wormhole Attack: In this type of attack, an attacker copies the whole packet or message by tunneling them to another network came from the originator. Then attacker transmits them to the destination node. When attacker transmits the copied messages or packets to the destination node, she/he transmits it speedily in such a way that copied packets reach to the destination node before the original packets (from legitimate user) reach there. To do that attacker uses *wormhole tunnel*. Wormhole nodes are fully invisible.

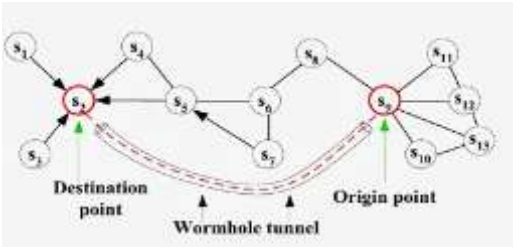

Figure 5 is a Worm Hole Attack on *Routing Protocols*

Adversary establishes a wormhole link between nodes s_9 and s_2, using a low-latency link. When node s_9 broadcasts its routing table as in distance vector routing protocols, node s_2 hears the broadcast via the wormhole and assumes is one hop away from s_2. Similarly, the neighbors of s_2 adjust their own routing tables and route via s_2 to reach any of the nodes s_9, $s_{10}s_{11}$, and s_{12}.

3.10. Sinkhole Attack: This is a special kind of selective forwarding attack which draws attention on the compromised node. Compromised node attracts all maximum possible traffic of the network. Then it places malicious node to the closest base station and it enables the selective forwarding attack. It is very complex attack. Detection of sinkhole attack is very hard and it affects the higher layer applications. Below figure illustrates the architecture of sinkhole attack.

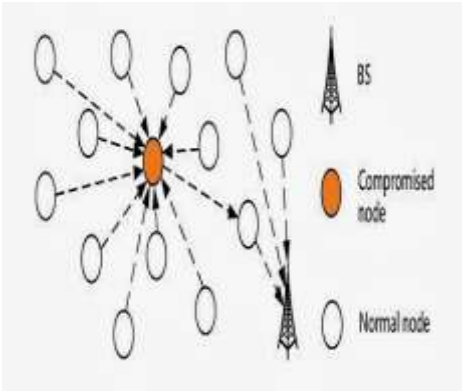

Figure 6 is a Sink Hole Attack on *Routing Protocols*

Interesting part is, sinkhole attack can be also done with wormhole attack. Below figure illustrates this scenario in which one malicious node gathers all traffic of the network *(sinkhole attack)* and it tunnels *(Wormhole attack)* with another node in order to reach to the base station.

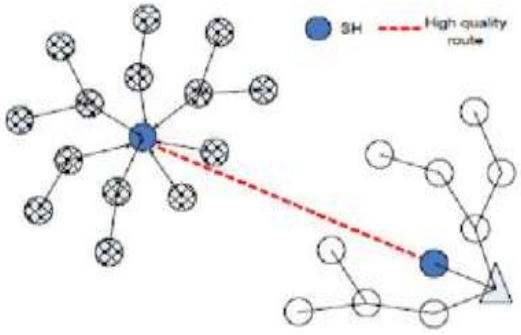

Figure 7 is a Sink Hole Attack

3.11. Impersonate Attack & Sybil Attack: This attack is very common and well known that attacker may obtain the legitimate person's IP address or MAC address in order to steal his/her identity and make it his/her own. Then attacker may attack another victim and can do plenty of things with that new stolen identity of legitimate user.In Sybil attack is an advanced version of impersonate attack in which malicious user attacker may steal multiple identities. In technical terms malicious node represents itself to the other fellow nodes by acquiring multiple identities within itself.

3.12. Traffic Analysis Attack: Here attacker gains the information of network traffic as well as behavior of the nodes. Traffic analysis can be done via checking the message length, pattern of message, duration in which it stayed within the session. Then attacker might correlate all these inbound and outbound traffic at any single custom router which might violate the privacy of the members due to being linked with those messages. Sometime attacker might able to link 2 nodes with unrelated connection within the network.

SECTION IV

4. Problem Definition: Now a days Wireless Networks became important, contains node. Communication through wireless networks when transmitting packet only few bytes of data may reach to destination other data corrupts beyond recovery by interfering with its jamming occurs. For example cell phone by transmitting a signal on the same frequency and at a high enough power that the two signals collide and cancel each other out. Cell phone are designed to add power if they experience low-level interference recognize the jammer and the match the power increase from the phone. Hiding the data is the solution to prevent the jamming node from identifying real time data ability to perform selective jamming.

4.1. Strong Hiding Commitment Scheme: Strong hiding commitment scheme which is based on symmetric cryptography. To satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. To satisfy the strong hiding property, the packet carrying d is formatted so that all bits of d are modulated in the last few *PHY* layersymbolsof the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d. We now present the implementation details of SHCS.

4.2. Cryptographic Puzzle Hiding Scheme: The implementation details which impact security and performance. Cryptographic puzzles are primitives 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. Proposed a construction called time-lock puzzles, which is based on the iterative application of a precisely controlled number of modulo operations. Time-lock puzzles have several attractive features such as the fine granularity in controlling tp and the sequential nature of the computation. Moreover, the puzzle

generation requires significantly less computation compared puzzling solving.

4.3. AONT Based Hiding Scheme: In this Module, 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.

4.4. Packet Hiding Technique: Packet-hiding techniques on the network performance via extensive simulations. To implement the hiding sub layer and measure its impact on the effective throughput of end-to-end connections and on the route discovery process in wireless ad-hoc networks. We chose a set of nodes running 802.11b at the PHY and MAC layers, AODV for route discovery, and TCP at the transport layer. Aside from our methods, we also implemented a simple MAC layer encryption with a static key. These packet-hiding methods require the processing of each individual packet by the hiding sub layer. We emphasize that the incurred processing delay is acceptable, even for real time applications. The SCHS requires the application of two permutations and one symmetric encryption at the sender, while the inverse operations have to be performed at the receiver.

4.5. Real time Packet Classification: In this module, once a packet is classified, the adversary may choose to jam it depending on his strategy. Consider the generic communication system depicted. 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, de-interleaved, and decoded, to recover the original packet m.

4.6. Selective Jamming Attacks: A jamming-resistant communication model for pair wise communications that does not rely on shared secrets. Communicating nodes use a physical layer modulation method called Uncoordinated Direct- Sequence Spread Spectrum (UDSSS). They also proposed a jamming-resistant broadcast method in which transmissions are spread according to PN codes randomly selected from a public codebook. Several other schemes eliminate overall the need for secret PN codes.

4.7. Evaluation: In our analysis we observe that a selective jamming attack against RREQ messages is equally effective to a constant jamming attack. However, selective jamming is several orders of magnitude more efficient. On the other hand, random jamming fails to disrupt the route discovery process due to the flooding mechanism of AODV.Not only symmetric and Brute force algorithm we can also apply machine learning algorithms to identify jammers in wireless networks.

SECTION V

5.Comparative Study: In previous workwireless 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 first the adversary has to expend a significant amount of energy to jam frequency bands of interest and second the continuous presence of unusually high interference levels makes this type of attacks easy to detect. Compare to existing work 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 attacksin 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.To mitigate such attacks, we develop three schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographicmechanisms with PHY-layer attributes. We analyze the security of our schemes and show that they achieve strong security properties, with minimal impact on the network performance.

CONCLUSION VI

Intrusion is an attack network communication internal adversary model in which the jammer is part of the network under attack thus being aware of the protocol specification and shared network secrets. Jammer attacks to transmit signals or communication from node to node packers in real time by decoding the first few symbols of an ongoing transmission. Our analysis presents the cryptography secure way to hide the data such as commitment schemes transformation and Comparative work with proposed system jammer can significantly impact performance with very that transform a selective jammer to a random one by prevent real time packet in efficient communication.

References

[1] AusCERT. AA-2004.02 - denial of service vulnerability in IEEE 802.11 wireless devices. http://www.auscert.org.

[2] J. Bellardo and S. Savage. 802.11 denial-of-service attacks: Real vulnerabilities and practical solutions. In *Proceedings of the USENIX Security Symposium*, pages 15{28, 2003.

[3] Brownfield, M.; Yatharth Gupta; Davis, N., "Wireless sensor network denial of sleep attack," Information Assurance Workshop, 2005. IAW '05. Proceedings from the Sixth Annual IEEE SMC , vol., no., pp.356,364, 15-17 June 2005

[4] Raymond, David R.; Midkiff, S.F., "Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses," Pervasive Computing, IEEE , vol.7, no.1, pp.74,81, Jan.-March 2008

[5] mister_x. (2011, 01 16). Aircrack-ng. Retrieved from http://www.aircrack-ng.org/doku.php?id=aircrack-ng

[6] Mustafa, H. (n.d.). THE SYBIL ATTACK IN SENSOR NETWORK.