Volume 3, Issue 8, August 2013 ISSN: 2277 128X

International Journal of Advanced Research in Computer Science and Software Engineering

Research Paper

Available online at: www.ijarcsse.com

Secure Transmission of Packets by Preventing Jamming Attacks

SaiDurga ShivaKumar Nuka
Dept of Computer Science & Eng
M.Tech, Software Engineering
Kakatiya Institute of Tech & Sci Kakatiya University
Warangal, India

Niranjan Reddy P
Dept of Computer Science & Eng
Professor & Head of CSE
Kakatiya Institute of Tech & Sci Kakatiya University
Warangal, India

Abstract-Built upon a shared wireless medium, wireless sensor network is particularly vulnerable to jamming attacks. These attacks can easily be accomplished by an adversary by either bypassing MAC-layer protocols or emitting a radio signal targeted at jamming a particular channel. This paper considers a scenario where a sophisticated jammer jams an area in a multichannel wireless sensor network. The jammer controls the probability of jamming and transmission range to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by a monitoring node in the network, and a notification message is transferred out of the jamming region. The jammer is detected at a monitor node by employing an optimal detection test based on the percentage of incurred collisions. Jamming makes itself known at the physical layer of the network, more commonly known as the MAC (Media Access Control) layer.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. To mitigate these attacks, we develop schemes that prevent real-time packet classification by combining cryptographic primitives with physical-layer attributes.

Index Terms—Wireless Networks, Cryptography, Packet Classification, Jamming Attacks

I. Introduction

The fundamental characteristic of wireless networks that renders them vulnerable to attacks is the broadcast nature of medium. This exposes them to passive and active attacks, which are different in their nature and objectives .In the former ones, the malicious entity does not take any action apart from passively observing the ongoing communication that is, eavesdropping with the intention to intervene with the privacy of network entities involved in the transaction. On the other hand, in active attacks the attacker is involved in transmission as well. If the attacker does not directly manipulate protocol parameters but exploits protocol semantics and aims at indirect benefits by unconditionally disrupting network operation, the attack is termed jamming or Denial-of-Service (DoS), depending on whether one looks at the cause or the consequences of it. Misbehavior in wireless networks stems from the selfish inclination of wireless network entities to improve their own derived utility at the expense of other nodes performance deterioration, by deviating from legitimate protocol operation at various layers.

Jamming can be as simple as sending out a strong noise signal over the wireless channel in order to prevent packets in the victim network from being received. Jamming gain is the increase in efficiency from exploiting features of the victim network relative to continuous jamming. More precisely, it is the amount of energy (or power as appropriate) used to achieve a desired effect relative to the amount of energy used to achieve the same effect with continuous jamming. This gain translates directly into reduced energy requirements for the attacker. At the link level, corrupting a single bit in a packet will cause the packet to fail its checksum and be discarded. For a 10,000 bit packet (1250 bytes) it implies that jamming gains as high as 40dB are possible. Further, typical wireless packet networks are lightly loaded so that jamming only when packets are present has further jamming gains. These examples make clear that there are significant jamming gains possible.

Targeted jamming refers to jamming only specific victim nodes, links, or flows. The attacker may be interested in only certain parts of the victim network, and attacking only these parts can lead to further jamming gains. With reduced probability of detection, the victim network may not realize that jamming countermeasures are necessary. Targeting some TCP-DATA packets will cause the TCP window to collapse and poor connection performance that a user might attribute to network congestion or a low quality wireless connection. Further, if ICMP packets are not blocked the victim users will have contradictory views of the network state. If jamming is discovered, lower probability of detection jamming will be harder to detect, localize, and suppress. Jamming is not a transmit-only activity. It requires an ability to detect and identify victim network activity, which we denote as sensing. At the physical layer a sensor needs to identify the presence of packets. Since the network is encrypted, only the start time and size of the packet can be measured. At higher layers a sensor needs to classify packets using protocol 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.

II. Related Work

We investigate the feasibility of real time packet classification for launching selective jamming attacks, under an internal threat model. We show that such attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes. We investigate the impact of selective jamming on critical network functions. Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer. The jammer controls the probability of jamming and transmission range to cause maximal damage to the network in terms of corrupted communication links. The jammer action ceases when it is detected by a monitoring node in the network, and a notification message is transferred out of the jamming region and the packets transferred over other route to the destination. To mitigate such attacks, we develop schemes that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes.

III. Problem Statement and Assumptions

Consider the scenario depicted in Fig. 1 Nodes A and B communicate via a wireless link. Within the communication range of both A and B there is a jamming node JN. When A transmits a packet to B, node J classifies packet by receiving only the first few bytes of packet. JN then corrupts it beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node JN from classifying packet in real time, thus mitigating JN jamming Node’s ability to perform selective jamming. Our goal is to transform a selective jammer to a random one. Note that in the present work, we do not address packet classification methods based on protocol semantics.

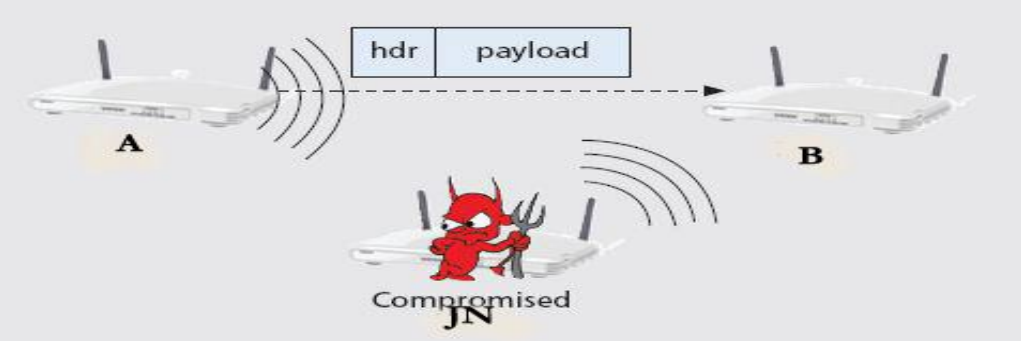

Fig. 1 Realization of selective jamming Attacks

Network model:-

The network consists of a collection of nodes connected over wireless links. Nodes may communicate directly if they are within the communication range or indirectly via multiple hops. Nodes are communicating either in unicast mode or broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all the intended receivers. These keys are provided using asymmetric cryptography. Inside a wireless network the Collection of nodes organized together requires a critical network function such as a neighbor discovery, routing, channel access and assignment and time synchronization. Control channels are the functions used in a broadcast communication medium that are coordinated by exchanging messages.

Adversary Model:-

We assume the adversary is in control of the communication medium and can jam messages at any part of the network. The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved by using multi radio transceivers. In addition, the adversary is equipped with directional antennas that enable the reception of a signal from one node and jamming of the same signal at another. Jammer can then decide to irrecoverably corrupt a transmitted packet by jamming the last symbol. In reality, it has been demonstrated that selective jamming can be achieved with far less resources.

Communication model:-

Consider the generic communication system depicted in Fig. 2. 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 which was sent by sender. The adversary’s ability in classifying a packet depends on the implementation details of the blocks in Fig. 2. The channel encoding block expands the original bit sequence m and adds necessary redundancy for protecting packet against channel errors. At the next block, interleaving is applied to protect packet from burst errors. Finally, the digital modulator maps the received bit stream to symbols of length q, and modulates them into suitable waveforms for transmission over the wireless channel. Typical modulation techniques include OFDM, BPSK, 16(64)-QAM and CCK.

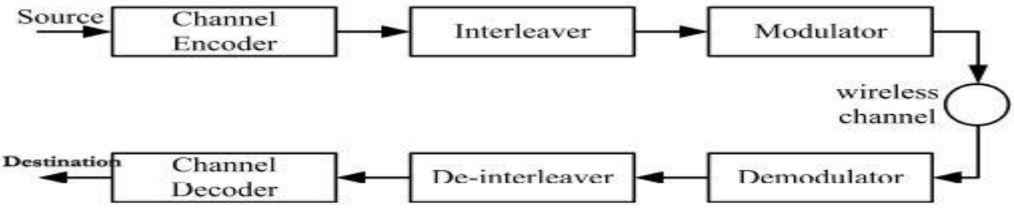

Fig. 2 Communication System Diagram

From our analysis, it is evident that intercepting the first few symbols of a packet is sufficient for obtaining relevant header information. For example, consider the transmission of a TCP-SYN packet used for establishing a TCP connection at the transport layer.

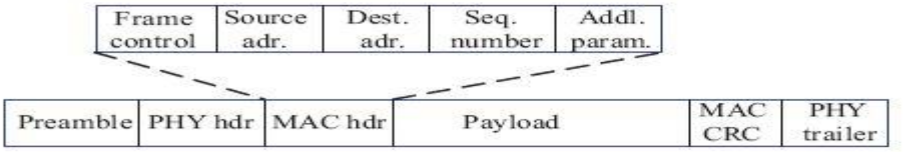

Fig. 3 Generic Frame format for a wireless Network

- Symbols 1-2 contain the PHY-layer header and the first byte of the MAC header. The PHY header reveals the length of the packet, the transmission rate, and synchronization information. The first byte of the MAC header reveals the protocol version and the type and subtype of the MAC frame (e.g., DATA, ACK).
- Symbols 3-10 contain the source and destination MAC addresses, and the length of the IP packet header.
- Symbols 11-17 contain the source and destination IP addresses the size of the TCP datagram carried by the IP packet, and other IP layer information. The first two bytes of the TCP datagram reveal the source port.
- Symbols 18-23 contain the TCP destination port, sequence number, acknowledgment number, TCP flags, window size, and the header checksum.
- Symbols 24-25 contain the MAC CRC code.

IV. System Architecture and Preventing Jamming Attacks

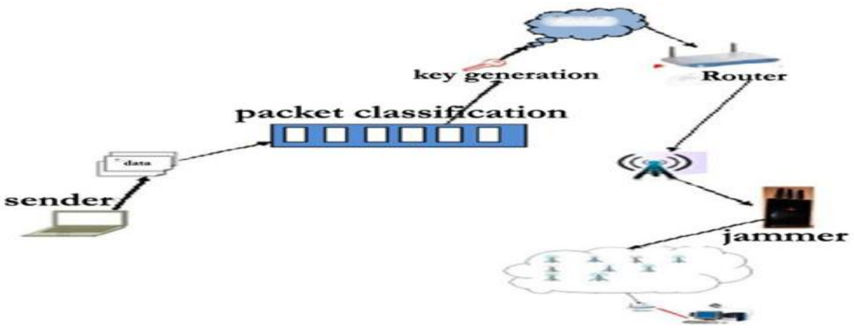

Fig. 4 System Architecture

The Source used to send the data packets to the Destination but in between the adversary tries to jam the selective packets by "Classify-and-then-jam" strategy. To avoid sender encrypt the data packet with and key which will append on the MAC layer of the packet also we use the Cryptographic primitives with time slot. Hence, only the destination can only decrypt the data packets and we use one more scheme Called "All-Or-Nothing Transformation" in which we used make the original packets into pseudo messages and when all the pseudo Message collected and decode we can get the original message therefore the adversary can function any attack on data packet on the fly in the wireless transmission. We used routing algorithm AODV for the routing in Ad-hoc network and encrypt the messages using cryptographic algorithm like AES. In the wireless networks we used to transmit data packets in the medium of air. Since it's a wireless medium a jammer can jam the signal using higher frequency and then jammer Decrypt the packet and gain the original data to avoid these attacks we proposed the three schemes which will able avoid the jamming attacks on the packet. Packet Classification is done by the jammer's they used to decrypt the packets on the fly they will know the source and destination of the packet and the content of the packet then they will corrupt the packet so that destination would receive corrupt packet and their data will be lost.

To avoid the error we used a Strong Hiding Commitment Scheme which are been used to store a strong key in the MAC layer of the packet. The key which is been generated are user defined, Source node define the key and append it on the packet and when the jammer tries the jam the packet. He can't retrieve the message since the key which stored in the packet. Cryptographic Puzzle Hiding Scheme are been develop to secure the packets which are been transferred in the vulnerable medium by append the puzzle in the packets at the PHY layer in the packet and then being transmitted. As we also append the time slot to crack the packet in the PHY layer when the jammer tries to jam the packet he cannot decrypt the packet within time slot as the destination might only now the answer for the puzzle. All-or-Nothing Transformation Based Hiding uses the Cryptographic primitives like AES and forms n Pseudo message hence when we collect all packets together then we decode it to get the original message. When a hacker tries to corrupt data he need to collect all the packets by just few pseudo packets we can decode the original message. The receiver used receives all the packets and then they decrypt the packet and get the original data; it is not possible by the jammers.

Strong Hiding Commitment Scheme

Strong Hiding: For every polynomial-time party V interacting with A and possessing pairs (C, dpart) and (C′, d′part), there is no (probabilistic) polynomially efficient algorithm that would allow V associate C with m and C′ with m′, with non-negligible probability. Here dpart and d′part are partial releases of d and d′, respectively, and the remaining parts of d and d′ are assumed to be secret. In the above definition, it is easily seen that the release of dpart must be limited to a fraction of d, in order for m to remain hidden. If a significant part of d becomes known to the verifier, trivial attacks, such as brute forcing the unknown bits of d, become possible.

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.

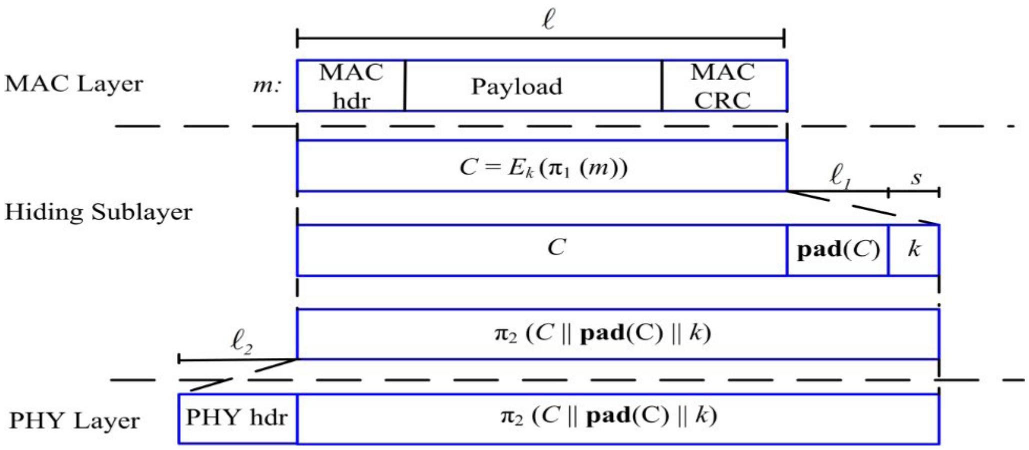

Fig. 5 Hiding sub layer

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. Here we used to have a jammer who tries to decrypt the packet on the fly. when the packets are been transmitted by an ordinary mode they can be easily decrypted by intentional interference attack but when we use the cryptographic primitives it can't be decrypted on the fly from source to destination. So we developed the three schemes for the secure data transmission on the vulnerable medium.

V. Evaluation of Secure Transmission of Packets

In this section, we evaluate the impact of our secure transmission of packet-hiding techniques on the network performance via extensive simulations. We used the OPNETTM Modeler to implement the hiding sublayer 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.

Impact on real-time systems– Our secure transmission of packet-hiding methods require the processing of each individual packet by the hiding sublayer. 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. Such operations can be implemented in hardware very efficiently. Symmetric encryption such as AES can be implemented at speeds of tens of Gbps/s when realized with

Application Specific Integrated Circuits (ASICs) or Field Programmable Gate Arrays (FPGAs). These processing speeds are orders of magnitude higher than the transmission speeds of most current wireless technologies, and hence, do not impose a significant delay. Similarly, the AONT-HS performs linear operations on the packet that can be efficiently implemented in hardware. We note that a non-negligible processing delay is incurred by the CPHS. This is due to the cryptographic puzzle that must be solved at the receiver. As CPHS should only be employed when the symbol size at the PHY layer is too small to support the SHCS and AONTHS solutions. The processing delays of the various schemes are taken into account in our experimental evaluations

Jamming attacks on voice communications have been launched since the 1940s. In the context of digital communications, the jamming problem has been addressed under various threat models. We present a classification based on the selective nature of the adversary. Prior Work on Selective Jamming In, Thuente studied the impact of an external selective jammer who targets various control packets at the MAC layer. To perform packet classification, the adversary exploits inter-packet timing information to infer eminent packet transmissions. In, Law et al. proposed the estimation of the probability distribution of inter-packet 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. Several researchers have suggested channel selective jamming attacks, in which the jammer targets the broadcast control channel. It was shown that such attacks reduce the required power for performing a DoS attack by several orders of magnitude. To protect control channel traffic, the replication of control transmission in multiple channels. The “locations” of the control channels where cryptographically protected. In, Lazos et al. proposed a randomized frequency hopping algorithm to protect the control channel from inside jammers. Strasser et al. proposed a frequency hopping anti-jamming technique that does not require the existence of a secret hopping sequence, shared between the communicating parties.

VI. Conclusion

Wireless Networks are prone to various external and internal security threats. While most external attacks can be mitigated with a combination of cryptographic mechanisms and robust communication techniques, internal attacks are much harder to counter because the adversary is aware of the network secrets and protocols. Jamming-resistant broadcast communications in the presence of inside jammers remains a challenging problem. Current solutions attempt to eliminate the use of common secrets for protecting broadcast communications. Such secrets can easily be exposed in the event of node compromise. However, the heightened level of security comes at the expense of performance, because broadcast messages have to be transmitted multiple times on multiple frequency bands to guarantee robust reception. Moreover, even if packet reception of critical messages is ensured, inside adversaries are in complete control of the traffic routed through them. A large body of literature addresses the problem of misbehavior in the form of packet dropping by developing reputation systems, credit-based systems, and communication-intensive acknowledgment schemes. Despite the relative wealth of literature on this problem, significant challenges are yet to be addressed. Most existing methods assume a continuously active adversary that systematically drops packets. These adversaries are detected by aggregate behavioral metrics such as per-packet reputation and credit. However, these metrics cannot detect attacks of selective nature, where only a small fraction of high-value packets is targeted. Furthermore, when the adversary drops only a few packets, his/her behavior can be indistinguishable from dropping patterns due to congestion or poor wireless conditions. Further challenges include efficient behavioral monitoring mechanisms that do not rely on continuous overhearing, and efficient maintenance and dissemination of reputation metrics.

References

[1]. A.Proano and L. Lazos, “Selective Jamming Attacks in Wireless Networks” Proc. IEEE ICC, 2010.

[2]. A.Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In *Proceedings of the Network and Distributed System Security Symposium*, pages 151–165, 1999.

[3]. W. Xu, W. Trappe, and Y. Zhang,“Anti-Jamming Timing Channels for Wireless Networks,” Proc. ACM Conf Wireless Network Security (WiSec),pp.203-213, 2008.

[4]. Y. Desmedt, “Broadcast Anti-Jamming Systems,” Computer Networks, vol. 35,nos. 2/3, pp. 223-236, Feb. 2001.

[5]. T. X. Brown, J.E. James, and A. Sethi,“Jamming and Sensing of Encrypted Wireless Ad Hoc Networks,” Proc.ACM Int’l Symp.Mobile Ad Hoc Networking and Computing(MobiHoc), pp. 120-130,2006.

[6]. A. Proano and L. Lazos, “Selective Jamming Attacks in Wireless Networks,” Proc. IEEE ICC, 2010.

[7]. Y. Zhang et al., “A Secure Incentive Protocol for Mobile Ad Hoc Networks,” Wireless Net., vol. 13, no. 5, 2007,

[8]. W. Xu, W. Trappe, Y. Zhang, T. Wood,"The feasibility of launching and detecting jamming attacks in wirelessnetworks", In Proceedings of the 6th ACM international symposium on Mobile Ad-Hoc networking and computing,

[9]. C. Karlof and D. Wagner. Secure routing in wireless sensor networks: attacks and countermeasures. In *Proceedings of the First IEEE International Workshop on Sensor Network Protocols and Applications*

[11]. L. Zhou and Z. Haas. Securing ad hoc networks. *IEEE Network*, 13(6):24{30, 1999.

[12]. H. Balakrishnan, S. Seshan, and R.H. Katz, “Improving reliable transport and handoff performance in cellular wireless networks,” *ACM/Baltzer Wireless Networks Journal,* vol. 1, no. 4