A Swarm Intelligence Algorithm to Prevent Selective Jamming Attacks in Wireless Network

[1]Gomathi S, [2]Aravindhan K
[1,2]Dept. of CSE, SNS College of Engineering, Coimbatore, Tamil Nadu, India

Abstract
Open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming. When intentional interference combined with wireless transmission it can be used as a launch pad for mounting denial-of-Service attacks on wireless networks. 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. Adversary active only for a short period of time selectively target messages of high importance. Selective jamming attacks can be launched by performing real-time packet classification at the physical layer. The jammer may decode the first few bits of a packet for recovering useful packet identifiers such as packet type, source and destination address. These attacks can be prevented by three schemes: commitment, cryptographic puzzle and AONTS. The combination of cryptographic primitives with physical layer attributes is used for preventing real-time packet classification and a swarm intelligence algorithm is used for preventing jamming attacks in wireless networks. Swarm intelligence algorithm is proficient enough to adapt changes in network topology and traffic. The sender and receiver change the channels in order to stay away from the jammer, in channel hoping technique.

Keywords
Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification, Swarm Intelligence, Channel Hopping

I. Introduction

Wireless networks are very less security due to the open nature of wireless medium. In wireless medium anyone can be eavesdrops the messages from the information channel. Here the jammer interrupts the communication between the two legitimate users. Signalling and control channels are essential to the operation of wireless networks. Such networks are constrained by the limited radio-frequency bandwidth and energy available to the mobile devices [1]. For an adversary agnostic to the implementation details of the network, a typical jamming strategy is the continuous emission of high-power interference signals such as continuous wave tones, or FM modulated noise [3]. However, adopting an "always-on" jamming strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presences of high interference levels make this type of jamming easy to detect [2,4,5]. Third, these attacks are easy to mitigate either by spread spectrum communications [3], spatial retreats [5], or localization and removal of the jamming nodes. In this paper, we consider a sophisticated adversary model in which the adversary is aware of the implementation details of the network protocols. By exploiting this knowledge, the adversary launches selective jamming attacks in which it targets specific packets of "high" importance. For example, jamming of TCP acknowledgments (ACKs) can severely degrade the throughput of a TCP connection due to the congestion control mechanism of the TCP protocol [3]. Compared to continuous jamming, the adversary is active for a short period of time, thus expending orders of magnitude less energy. To perform selective jamming, the adversary must be capable of classifying transmitted packets in real time, and corrupting them before the end of their transmission. Packet classification can be performed by receiving just a few bytes of a packet, for example, by decoding the frame control field of a MAC-layer frame.

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 [13]. Such strategy can be actualized either by classifying transmitted packets using protocol semantics [10], [14], or by decoding packets on the fly [9]. 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 [9]. Selective jamming requires an intimate kno
wledge of the physical (PHY) layer, as well as of the specifics of upper layers. Swarm Intelligence (SI) is all about designing intelligent multi-agent systems inspired by collective activities of social insects such as ants, bees and wasps. The agents in the SI system interact directly or indirectly in a distributed troubleshooting way. The agents move towards for the optimal results and interact directly by sharing facts with their neighbours [12]. These agents are very helpful in finding the minimum path to the concerned destination in a short time required.

II. Related Works

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s [3]. Recently, several alternative jamming strategies have been demonstrated [2], [12], [4], [5]. Xu et. al. jammers Categorized into four models, (i) a constant jammer that continuously emits noise, (ii) a deceptive jammer that continuously broadcasts fabricated messages , (iii) a random jammer that alternates between periods of an active mode and inactive mode, (iv) a reactive jammer who jams only when transmission action is detected. Intelligent attacks which aim the transmission of specific packets were presented in [8], [18]. Thuente considered an attacker who infers eminent packet transmissions based on timing information at the MAC layer

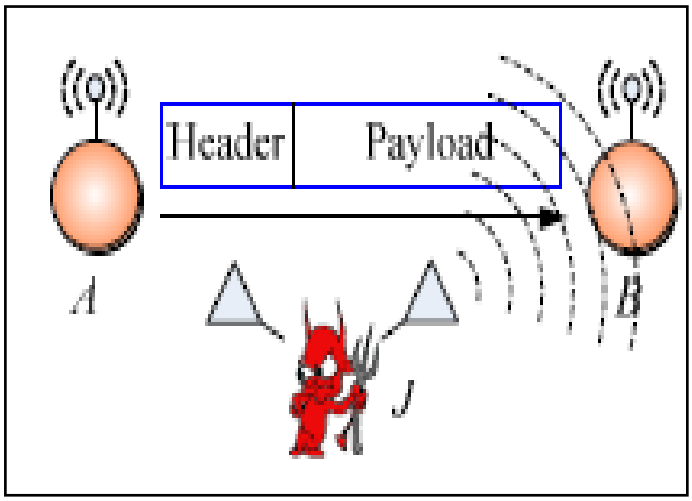

Fig. 1(a): Realization of a Selective Jamming Attack

When radio devices communicate they operate on a single channel. When an adversary comes in range and blocks the use of a specific channel, it is natural to migrate to another channel [5]. The idea of channel surfing is motivated by a common physical layer technique known as frequency hopping. When mobile nodes are interfered with, they should simply move to a safe location. Spatial retreat is often a desirable defense strategy to employ since most wireless networks involve mobile participants, such as users with cell phones or WLAN enabled laptops.

III. Methology

A. Network Model

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using preshared, pair wise keys or asymmetric cryptography.

B. Adversary Model

The adversary is in control of the communication medium and can jam messages at any part of the network of his choosing (similar to the Dolev- Yao model). The adversary can operate in full-duplex mode, thus being able to receive and transmit simultaneously. This can be achieved, for example, with the use of 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. In reality, it has been demonstrated that selective jamming can be achieved with far less resources [8-9]. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. However, our model captures a more potent adversary that can be effective even at high transmission speeds.

The adversary is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. Solving well-known hard cryptographic problems is assumed to be time-consuming. For the purposes of analysis, given a cipher text, the most efficient method for deriving the corresponding plaintext is assumed to be an exhaustive search on the key space. The implementation details of every layer of the network stack are assumed to be public. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc.

C. Strong Hiding Commitment Scheme (SHCS)

Strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. The motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. 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. To achieve the strong hiding property, a sublayer called the "hiding sublayer" is inserted between the MAC and the PHY layers. This sublayer is responsible for formatting m before it is processed by the PHY layer. A frame m at the MAC layer delivered to the hiding sublayer. Frame m consists of a MAC header and the payload, followed by the trailer containing the CRC code. 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.

D. Cryptographic Puzzle Hiding Scheme (CPHS)

We use cryptographic puzzles to temporary hide transmitted packets. A packet m is encrypted with a randomly selected key k of a desirable length s. The key k is blinded using a cryptographic puzzle and sent to the receiver. For a computationally bounded adversary, the puzzle carrying k cannot be solved before the transmission of the encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming.

Several client puzzle schemes have been created in which the client is asked to reverse a cryptographic hash function. Because hash functions are one-way functions, brute forcing the reverse is computationally hard. To counter this Juels and Brainard [8] provide a part of the reverse as the puzzle and let the client look for the remaining l bits.

1. Setup (l): mk is a server secret, h() is the chosen hash function and params = f ` ; h()g.
2. PuzzleGen(mk; req): req contains the request message M. Let t be the current time. This information is hashed together with the server secret to form the basis of the puzzle, x = h(mk; t;M). The _rst l bits, the pre_x, of x are replaced by 0 to form x0. The output is puz = fx0; h(x); t;Mg and info = ;.
3. PuzzleSol(puz): The pre_x of x0 is replaced with another bit string to form a candidate solution z. When ignoring the pre_x of z and x, z is equal to x. This candidate solution is checked using h(z) =? h(x). When the right value is found, this algorithm outputs the solution sol = fz; t;Mg.
4. PuzzleVer(info;mk; sol): _rst check that t is a recent timestamp. If this is not the case, the solution is rejected. Otherwise it is checked with z =? h(mk; t;M)

E. All-or-Nothing Transformation (AONT)

The proposed a solution based on all-or-nothing Transformations that introduces a modest communication and computation overhead. Such transformations were originally proposed by Rivest to slow down brute force attacks against block encryption algorithms packets are preprocessed 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 An AONT serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm. A transformation f, mapping message m= {m1; . . .;mx } a sequence of pseudo messages a plaintext is pre-processed by an AONT before encryption, all cipher text blocks must be received to obtain any part of the plaintext. Therefore, brute force attacks are slowed down by a factor equal to the number of cipher text blocks, without any change on the size of the secret key.

F. Swarm Intelligence Technique

Jamming can interrupt wireless transmission and occur by mistake in form of interference, noise or as collision at the receiver or in the circumstance of an attack. In this paper, we propose a swarm based defense technique for jamming attacks in wireless sensor networks. Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic. The sender and receiver change channels in order to stay away from the jammer, in channel hoping technique. The jammers remain on a single channel, hoping to disrupt any fragment that may be transmitted in the pulse jamming technique. Using the swarm intelligence technique, the forward ants either unicast or broadcast at each node depending on the availability of the channel information for end of the channel. If the channel information is available, the ants randomly choose the next hop. As the backward ants reaches the source, the data collected is verified which channel there is prevalence of attacker long time, and those are omitted. Simultaneously the forward ants are sent through other channels which are not detected before for attacks. In this paper to implement the intelligence techniques using the ant colony optimization. This scheme helps limit the channel maintenance overhead.

IV. Performance Evaluation

We set up a single file transfer between a sender and receiver, connected via a multihop route. The receiver requested a 1MB file from the sender. The delay is defined as the time difference between the transmission of the first RREQ from a source and the reception of the corresponding RREP from the destination. We observe that the impact of packet hiding on the route discovery delay is minimal compared to the case where no packet hiding is employed. This similarity in performance is due to the expanding ring search technique of AODV, Which is used to prevent unnecessary network-wide dissemination of RREQs. Here using swarm intelligence technique to improve the packet delivery ratio and reduce the jamming attacks.

V. Conclusion

Packet hiding methods addressed the problem of selective jamming attacks in wireless networks. Hiding methods 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.The jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. Evaluated the impact of selective jamming attacks on network protocols such as TCP and routing. This method shows that a selective jammer can significantly impact performance with very low effort. The three schemes that transform a selective jammer to a random one by preventing real-time packet classification. The cryptographic scheme in packet hiding methods increases computation complexity and AONTS consumes more delay. To overcome this limitation, a swarm based defense technique for jamming attacks in wireless networks. Swarm intelligence algorithm is proficient enough to adapt change in network topology and traffic. Using the swarm intelligence technique, the forward ants either unicast or broadcast at each node depending on the availability of the channel information for end of the channel.

References

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

[2] G. Noubir, G. Lin,"Low-power DoS attacks in data wireless LANs and countermeasures", ACM SIGMOBILE Mobile Computing and Communications Review, 7(3), pp. 29–30, 2003.

[3] M. Simon, J. Omura, R. Scholtz, B. Levitt,"Spread spectrum communications handbook", McGraw-Hill Companies, 1994.

[4] W. Xu, W. Trappe, Y. Zhang, T. Wood,"The feasibility of launching and detecting jamming attacks in wireless networks", In Proceedings of the 6th ACM international symposium on Mobile Ad-Hoc networking and computing, pp. 46–57, 2005.

[5] W. Xu, T. Wood, W. Trappe, Y. Zhang,"Channel surfing and spatial retreats: Defenses against wireless denial of service", In Proceedings of the 3rd ACM workshop on Wireless security, pp. 80–89, 2004.

[6] I. Damgard,"Commitment schemes and zero-knowledge protocols", Lecture notes in computer science, 1561, pp. 63–86, 1999

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

[8] B. Thapa, G. Noubir, R. Rajaramanand, B. Sheng,"On the robustness of IEEE802.11 rate adaptation algorithms against smart jamming", In Proceedings of WiSec, 2011.

[9] M. Wilhelm, I. Martinovic, J. Schmitt, V. Lenders. Reactive jamming in wireless networks: How realistic is the threat?", In Proceedings of WiSec, 2011.

[10] G. Noubir, G. Lin,"Low-Power DoS Attacks in Data Wireless Lans and Countermeasures", Mobile Computing and Comm. Rev., Vol. 7, No. 3, pp. 29-30, 2003.

[11] C. Perkins, E. Belding-Royer, S. Das,"RFC 3561: Ad Hoc On- Demand Distance Vector (AODV) Routing", Internet RFCs, 2003.

[12] Periyanayagi S., Sumathy V.,"A Swarm Based Defense Technique for Jamming Attacks in Wireless Sensor Network", International Journal of Computer Theory and Engineering, Vol. 3, No. 6, 2011.

[13] Alejandro Proano, Loukas Lazos,"Packet Hiding Methods for Preventing Selective Jamming Attacks", Vol. 9, No. 1, pp. 101-114, 2012.

[14] D. Thuente, M. Acharya, "Intelligent Jamming in Wireless Networks with Applications to 802.11 b and Other Networks," Proc. IEEE Military Comm. Conf. (MILCOM), 2006.

GOMATHI S. received BE degree in computer science and Engineering from Anna University Chennai, Tamil Nadu, India in 2011.She is currently pursuing her M.E in Computer Science and Engineering from SNS College of engineering, Coimbatore .Her research interest include Networking, Cryptographic and Network Security.

ARAVINDHAN K. received BE degree in computer science and engineering from anna university Chennai in 2007 and ME degree in computer science and engineering from Kumaraguru College of Technology, Coimbatore in 2009. Presently he is working as Assistant Professor in Department of Computer Science and Engineering, SNS College of Engineering, Coimbatore, Tamil Nadu. His area of interest includes Wireless Sensor Network, VANET, and Network Security.