Secured Routing of Data In Wireless Network Based On Packet Hiding Methodology

Rini Vijayan
Department of Computer Science and Engineering
Sarabhai Institute Of Science And Technology
Trivandrum
rini.vij@gmail.com

Abstract— **The open nature of the wireless medium is always vulnerable to intentional interference attacks, referred to as jamming. This jamming can be used as a launch pad for mounting Denial-of-Service attacks on wireless networks.Typically,jamming has been addressed under an external threat model. In this work, the problem of selective jamming attacks is addressed under an internal threat model. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. To mitigate these attacks, three schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes are used . In this paper, we study the problem of identifying the maximum available bandwidth path, a fundamental issue in supporting quality-of-service by using a new path weight mechanism which captures the available path bandwidth information . Hop-by-hop routing protocol based on the new path weight satisfies the consistency and loop-freeness requirements.**

Keywords—Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification

I. INTRODUCTION

Network security is of great importance because of intellectual property that can be easily acquired through the internet. With the advent of the internet, security became a major concern and the history of security allows a better understanding of the emergence of security technology. The internet structure itself allowed for many security threats to occur. An effective network security plan is developed with the understanding of security issues, potential attackers, needed level of security, and factors that make a network vulnerable to attack.

The open nature of wireless 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 several short jamming pulses . Typically, jamming attacks[1] have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high power interference signals .However, adopting an "always-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect .

Conventional anti-jamming techniques are based on spread-spectrum[8] communications or some form of jamming evasion. SS techniques provide bit-level protection by spreading bits according to a secret pseudo noise code, Known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions.

In this paper, the problem of selective jamming attacks is addressed under an internal threat model.Here jamming is created by 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.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 .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 attacks requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers. Selective jamming attacks lead to a DoS with very low effort on behalf of the jammer. To mitigate such attacks, three schemes that prevent classification of transmitted packets in real time are developed. These schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes.

II. PRELIMINARIES

Conventional anti-jamming techniques relies extensively on spread-spectrum communications. SS techniques provide bit-level protection by spreading bits according to a secret pseudo noise code, known only to the communicating parties. These methods can only protect wireless transmissions under an external threat model. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions.This strategy has several disadvantages. First ,the broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.Second,the continuous presence of unusually high interference levels makes this type of attacks easy to detect. Potential disclosure of secrets due to node compromise neutralizes the gains of SS

III.PROBLEM FORMULATION

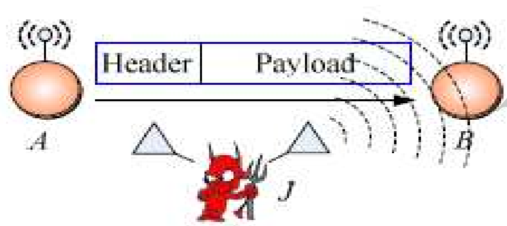

Fig 1.Realization of a selective jamming attack

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 J. When A transmits a packet m to B, node J classifies m by receiving only the first few bytes of m. J then corrupts m beyond recovery by interfering with its reception at B. The problem of *preventing the jamming node from classifying* m *in real time, thus mitigating* J*'s ability to perform selective jamming* is addressed.

IV. PROPOSED SYSTEM

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, three schemes that prevent classification of transmitted packets in real time is considered. These schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. Also propose a new path weight that captures the concept of available bandwidth. It gives the mechanism to compare two paths based on the new path weight and develop a hop-by-hop packet forwarding scheme. The isotonicity property of the proposed path weight allows us to develop a routing protocol that can identify the maximum bandwidth path from each node to each destination. In particular, it tells us whether a path is worthwhile to be advertised, meaning whether a path is a potential subpath of a widest path.

V. HIDING BASED ON COMMITMENTS

The problem of real-time packet classification is mapped to the hiding property of commitment schemes, and propose a packet-hiding scheme based on commitments.

A. Strong Hiding Commitment Scheme (SHCS)

SHCS is based on symmetric cryptography Assume that the sender has a packet for Receiver. First, S constructs (C, d) = commit (m), where, $C = E_k(\pi 1(m))$, d = k. Here, the commitment function $E_k()$ is an off-the-shelf symmetric encryption algorithm (e.g., DES or AES), $\pi 1$ is a publicly known permutation, and $k \in \{0, 1\}s$ is a randomly selected key of some desired key length s (the length of k is a security parameter). The sender broadcasts (C||d), where "||" denotes the concatenation operation. Upon reception of d, any receiver R computes

$$m=\pi_1^{-1}(D_k(C)),$$

where π^{-1} denotes the inverse permutation of π_1. 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 layer symbols of the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d.

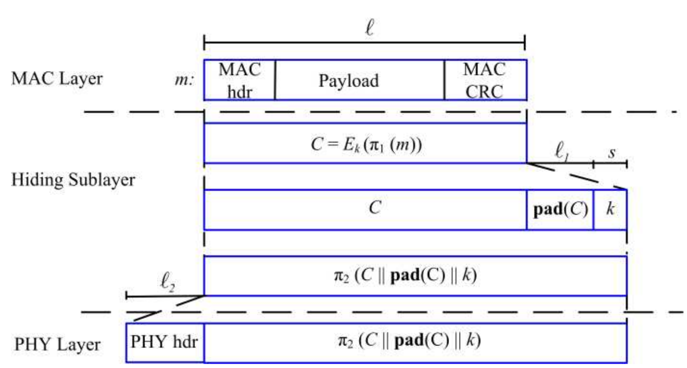

Fig 2. Processing at the hiding sublayer

Consider 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. Initially, m is permuted by applying a publicly known permutation $\pi 1$. The purpose of $\pi 1$ is to randomize the input to the encryption algorithm and delay the reception of critical packet identifiers such as headers. After the permutation, $\pi_1(m)$ is encrypted using a *random* key k to produce the commitment value $C = E_k(\pi_1(m))$. Although the random permutation of m and its encryption with a random key k seemingly achieve the same goal . In the next step, a padding function **pad**() appends **pad**(C) bits to C, making it a multiple of the symbol size. Finally, C||**pad**(C)||k is permuted by applying a publicly known permutation π_2. The purpose of π_2 is to ensure that the interleaving function applied the PHY layer does not disperse the bits of k to other symbols.

B. Cryptographic Puzzle Hiding Scheme (CPHS)

This scheme is based on cryptographic puzzles[3]. 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.

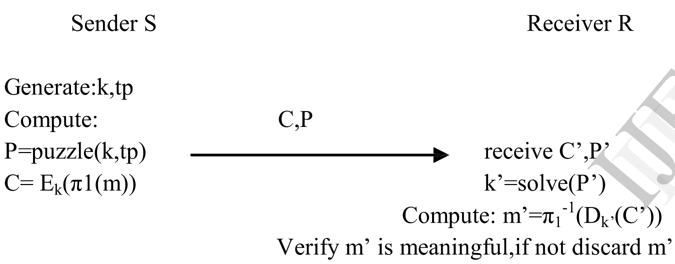

Fig 3. Cryptographic puzzle based hiding scheme

C. All-Or-Nothing Transformation(AONT)

An AONT[9] serves as a publicly known and completely invertible pre-processing step to a plaintext before it is passed to an ordinary block encryption algorithm. The packets are pre-processed by an AONT before transmission but remain unencrypted. Packet m is partitioned to a set of x input blocks $m = \{m_1, . . . ,m_x\}$, which serve as an input to an AONT $f: \{F_u\}x \rightarrow \{F_u\}x'$. Here, Fu denotes the alphabet of blocks mi and x′ denotes the number of output pseudo-messages with $x' \geq x$.The set of pseudo-messages $m' = \{m'_1, . . . ,m'_x\}$ is transmitted over the wireless medium. At the receiver, the inverse transformation f^{-1} is applied after all x′ pseudo-messages are received, in order to recover m.

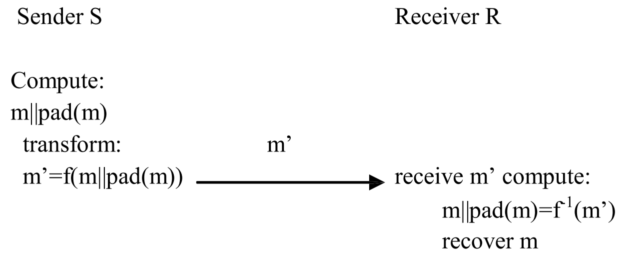

Fig 4.The AONT-Based Hiding Scheme

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. A transformation f, mapping message $m = \{m_1, \cdot \cdot \cdot ,m_x\}$ to a sequence of pseudo-messages $m' = \{m'_1, \cdot \cdot \cdot ,m'_x\}$, is an AONT if (a) f is a bijection (b) it is computationally infeasible to obtain any part of the original plaintext, if one of the pseudo-messages is unknown. Under this model, all plaintexts are equiprobable in the absence of at least one pseudo-message.

AONT-HS is implemented at the hiding sublayer residing between the MAC and the PHY layers. In the first step, m is padded by applying function pad() to adjust the frame length so that no padding is needed at the PHY layer, and the length of m becomes a multiple of the length of the pseudo-messages m'_i. This will ensure that all bits of the transmitted packet are part of the AONT. In the next step, m||pad(m) is partitioned to x blocks, and the AONT f is applied. Message m′ is delivered to the PHY layer. At the receiver, the inverse transformation f^{-1} is applied to obtain m||pad(m). The padded bits are removed and the original message m is recovered. The steps of AONT-HS are shown in Fig. 4.

D. Path Selection

This scheme propose a new path weight that captures the concept of available bandwidth[11] .It focuses on the problem of identifying the maximum available bandwidth path from a source to a destination, which is also called the Maximum Bandwidth Problem (MBP). MBP is a sub problem of the Bandwidth-Constrained Routing Problem (BCRP), the problem of identifying a path with at least a given amount of available bandwidth . Maximum available bandwidth path is also called widest path. Given a path p <v1; v2; . . . ; vh>, based on the current flows on each link in the network, denote B(e) as the available bandwidth of link e. Denote Qp as the set of the maximal cliques containing only the links on p. The available bandwidth of path p is estimated as follows :

$$B(p) = \min_{q \in Q_p} C_q \quad (1)$$

$$C_q = \frac{1}{\sum_{l \in Q} \frac{1}{B(l)}} \quad (2)$$

Cq is thus the bandwidth available over the clique q. The available bandwidth of the path is the bandwidth of the bottleneck clique.

VI.EXPERIMENTAL EVALUATION

When a single file is transfered between a client and server, connected via a multi-hop route. The effects of packet hiding can be evaluated by measuring the effective throughput of the TCP connection in the following scenarios: (a) No packet hiding (b) SHCS (c) Time-lock CPHS (d)AONT-HS based on the package transform.

Here SHCS achieves an effective throughput close to the throughput in the absence of packet hiding. The AONT-HS based on the package transform achieved slightly lower throughput, because it occurs a per-packet overhead of 128 bits as opposed to 56 bits for SHCS.The hiding techniques based on cryptographic puzzles decrease the effective throughput of the TCP connection to half, compared to the no hiding case. This performance is anticipated since the time required to solve a puzzle after a packet has been received at the MAC layer is equal to the transmission time of each packet. The efficient packet-hiding techniques such as SHCS, and AONT-HS have a relatively small impact on the overall throughput. This is because in a congested network, the performance is primarily dependent on the queueing delays at the relay nodes. The communication overhead introduced by the transmission of the packet hiding parameters is small and hence, does not significantly impact the throughput. On the other hand, for CPHS, a performance reduction of 25% − 30% compared to the case of no packet-hiding. This reduction is attributed to the delay introduced by CPHS for the reception of each packet. In the congested network scenario, the throughput reduction of CPHS is smaller compared to the non-congested one because nodes can take advantage of the queuing delays to solve puzzles.

VII.CONCLUSION

The selective jamming attacks can be launched by performing real-time packet classification at the physical layer. A selective jammer can significantly impact performance with very low effort.The proposed system develops three schemes that transform a selective jammer to a random one by preventing real-time packet classification. These schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations (AONTs) with physical layer characteristics.First the problem of real-time packet classification can be mapped to the hiding property of commitment methods and propose a packet-hiding method based on commitments. Second a packet-hiding method based on cryptographic puzzles. Finally All -or- Nothing Transformations that introduces a modest communication and computation overhead. This paper also explains the maximum available bandwidth path problem, which is a fundamental issue to support quality-of-service. It focuses on the problem of identifying the maximum available bandwidth path from a source to a destination by determining the maximal clique in the conflict graph. Based on the available path bandwidth information, a source can immediately determine some infeasible connection requests with the high bandwidth requirement.In future we can gather the Jamming node information on the server where as, here we have done on the client side.

ACKNOWLEDGMENT

It is with great pleasure and learning spirit that I am bringing out this paper. I use this opportunity to express my heartiest gratitude to the support and guidance offered to me from various sources.

I am extremely grateful to the Head of Institution Dr. M K Jana, Sarabhai Institute of science and Technology, Vellanad for providing necessary facilities. We are grateful to our Head of the Department Dr. C.G. Sukumaran Nair or valuable suggestions.

I also wish to thank all our faculties of Computer Science and Department for their proper guidance and help.

Above all, I owe my gratitude to Almighty for showering abundant blessings upon me. And last but not the least I wish to thank my parents and my friends for helping me to prepare this paper.

REFERENCES

[1] Alejandro Proano And Loukas Lazos January/February 2012 "Packet Hiding Methods for Preventing Selective Jamming Attacks "IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (vol. 9 no. 1)

[2] 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

[3] R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timed release crypto.Massachusetts Institute of Technology, 1996

[4] A.Chan,X.Liu.G.Naubir and B.Thapa. Control Channel Jamming: Resilience and identification of traitors. In *Proceedings of ISIT*, 2007

[5] Liang Xiao,Huaiyu Dai,Peng Ning. Jamming-resistant broadcast communication using uncoordinated frequency hopping. In Proceedings of the USENIX Security Symposium, 2009.

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

[7] Serge Vaudney. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978.

[8] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.

[9] R. Rivest. All-or-nothing encryption and the package transform Lecture Notes in Computer Science, pages 210–218, 1997.

[10] Y.Yang and R.Kravets,"Contention-Aware Admission Control for Adhoc Networks,"IEEE Trans.Mobile Computing,vol.4,no.4,pp. 363-377, Apr. 2009.

[11] Ronghui Hou, King-Shan Lui, Fred Baker, and Jiandong Li. Hop-by-Hop Routing in Wireless Mesh Networks with Bandwidth Guarantees,2012

[12] Y. Desmedt. Broadcast anti-jamming systems. *Computer Networks*,35(23):223–236, February 2001.

[13] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES.*Cryptographic Engineering*, pages 235–294, 2009.

[14] O. Goldreich. *Foundations of cryptography: Basic applications*. Cambridge University Press, 2004.

[15] Z. Jia, R. Gupta, J. Walrand, and P. Varaiya, "BandwidthGuaranteed Routing for Ad-Hoc Networks with Interference Consideration," Proc. IEEE Symp. Computers and Comm., pp. 3-9,2005.

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

[16] W. Xu, W. Trappe, and Y. Zhang. Anti-jamming timing channels for wireless networks. In *Proceedings of WiSec*, pages 203–213, 2008.

[17] W. Xu, W. Trappe, Y. Zhang, and T.Wood. The feasibility of launching and detecting jamming attacks in wireless networks. In *Proceedings of MobiHoc*, pages 46–57, 2005.

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

[19] X. Cheng, P. Mohapatra, S.-J. Lee, and S. Banerjee, "MARIA: Interference-Aware Admission Control and QoS Routing in Wireless Mesh Networks," Proc. IEEE Int'l Conf. Comm. (ICC '08), pp. 2865-2870, May 2008.

[20] M. Kodialam and T. Nandagopal, "Characterizing the Capacity Region in Multi-Radio Multi-Channel Wireless Mesh Networks," Proc. ACM MobiCom, pp. 73-87, Aug. 2005.

[21] IEEE.IEEE802.11standard. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007

[22] A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151-165, 1999.

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

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