Survey on Packet Hiding Scheme for Network Security by Selective Jamming Attacks

Katkar Kiran B., Dukare Ajay B., Pawar Monali R., Darandale Dnyaneshwar R.

***Abstract*—*In the network environment most of the time there could be more chances of the attacks. That means most of the time does not guarantee about the packets can be easily transfer over the network. It affects network performance degrade. To overcome the above problem of network traffic and performance implementing a Packet Hiding Scheme that can be securely sent packets over the network. 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 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 have been considered under an external threat model, in which the jammer is not part of the network. In this paper we are developing and survey on the three schemes that prevent real-time packet classification by combining Cryptographic Puzzles, SHCS, AONT. We analyze the security of our methods and evaluate their computational and system overhead.*

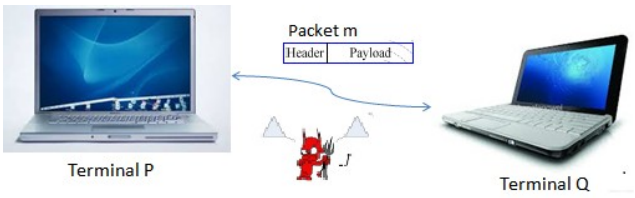
***Index Terms*—**Brute force attack, Denial of Services, Encryption, Jammer.

I. INTRODUCTION

In this paper, we are addressing 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 implementing a "classify-then-jam" strategy before the completion of a network transmission. Conventional anti-jamming techniques were used on spread-spectrum (SS) communications, or some form of jamming evasion. SS techniques provide bit-level protection according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect network transmissions under the external threat model.

In this paper, we are addressing the problem of jamming under an internal threat model. We consider a sophisticated model that is aware about network secrets and the implementation details of network protocols at any layer in the network. The model uses its internal knowledge for launching selective jamming attacks in which specific messages of "high importance" are targeted. Packet uses the identifiers such as packet type, source and destination address. After classification, model must induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver . Preventive Selective jamming technique requires an knowledge of the physical (PHY) layer, network layer as well as transport layer[1][2].

II. PROBLEM STATEMENT



Consider the Figure 1 Terminal P and Q communicate with network. Within the communication range of both P and Q there is a jamming node J. When P transmits a packet m to J, node J (jammer) classifies m packets by receiving only the first few bytes of m. Jammer J then corrupts m packet beyond recovery by interfering with its reception at Q.

III. EXISTING SYSTEM

Conventional anti-jamming techniques were based on spread-spectrum (SS) communications. SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model [1].

In the network environment most of the time there could be more chances of the attacks. That means most of the time does not guarantee about the packets can be easily transfer over the network. It affects network performance degrade.

A)Disadvantages of Existing System

1)Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions [1].
2)The open nature of the wireless medium leaves it vulnerable to intentional interference attacks, typically referred to as jamming [1].
3)Anyone with a transceiver can eavesdrop on network transmissions, inject spurious messages, or jam legitimate ones. Hence, the compromise of a single receiver is sufficient to reveal relevant cryptographic information.

IV.PROPOSED SYSTEM

An intuitive solution to selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification.

A) Advantages of Existing System

1) Relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes [1].

2) Our findings indicate that selective jamming attacks lead to a (DoS) with very low effort on behalf of the jammer.

3) Achieve Strong Security properties.

V. SYSTEM MODELS

A) Normal mode Transmission:

In this mode the data transmitted from client to server with block or unblock mode, because in this mode does not have any security measures therefore data successfully transmitted via unblock mode and fail via blocked mode.

B) Strong Hiding Commitment Scheme:

A Strong Hiding Commitment Scheme (SHCS), which is based on symmetric cryptography. Assume that the sender has a packet for receiver. First, S constructs commit(message)the commitment function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is a randomly selected key of some desired key lengths (the length of k is a security parameter). Upon reception of d, any receiver R computes[3].

C) Cryptographic Puzzle:

A sender S has a packet m for transmission. The sender selects a random key k, of a desired length. S generates a puzzle (key, time), where puzzle () denotes the puzzle generator function, and type denotes the time required for the solution of the puzzle. Parameter is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second. After generating the puzzle P, the sender broadcasts (C, P). At the receiver side, any receiver R solves the received puzzle to recover key and then computes[1].

D)All-Or-NothingTransformations:

The 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. Packet m is partitioned to a set of x input blocks m = {m1, m2, m3….}, which serve as an input to an The set of pseudo-messages m = {m1, m2, m3,…..} is transmitted over the medium[1].

VI. CASE STUDIES

Thuente and *Acharya* 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[3].

In Law et al. Proposed the estimation of the probability distribution 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.

Brown et al. illustrated the feasibility of selective jamming based on protocol semantics. They considered several packet identifiers for encrypted packets such as packet size, precise timing information of different protocols, and physical signal sensing. To prevent selectivity, the unification of packet characteristics such as the minimum length and inter packet timing was proposed. Similar packet classification techniques were investigated.

Liu et al. considered a smart jammer that takes into account protocol specifics to optimize its jamming strategy. The adversary was assumed to target control messages at different layers of the network stack. To mitigate smart jamming, the authors proposed the SPREAD system, which is based on the idea of stochastic selection between a collection of parallel protocols at each layer.

The uncertainty Introduced by this stochastic selection mitigated the selective ability of the jammer. Greenstein et al. Presented at 802.11-like wireless protocol called Slyfi that prevents the classification of packets by external observers. This protocol hides all explicit identifiers from the transmitted packets (e.g., MAC layer header and payload), by encrypting them with keys only known to the intended receivers.

Selective jamming attacks have been experimentally implemented using software-defined radio engines. Wilhelm et al. implemented a USRP2-based jamming platform called Refract that enables selective and reactive jamming. Refract was shown to be agnostic to technology standards and readily adaptable to any desired jamming strategy. The success rate of a selective jamming attack against a 802.15.4 network was measured to be 99.96 percent.

Thana et al. studied selective jamming attacks against the rate-adaptation mechanism of 802.11 they showed that a selective jammer targeting specific packets in a point-to-point 802.11 communication was able to reduce the rate of the communication to the minimum value of 1 Mbps, with relatively little effort (jamming of five to eight packets per second).
They also proposed a jamming-resistant broadcast method in which transmissions are spread according to PN codes randomly selected from a public code book. Several other schemes eliminate the overall need for secret PN codes. Lin and Noubir showed that jamming 13 percent of a packet is sufficient to overcome the ECC capabilities of the receiver. Xu et al. categorized jammers into four models:
1) A constant jammer.
2) A deceptive jammer that broadcasts messages.
3) A random jammer.
4) A reactive jammer that jams only if activity is sensed.

VII. SYSTEM FEATURES

1) FEATURE:
In order To send the file to destination the user browse the particular file present on his system and then click on selection node this node having its own number though which data transmission happens and choose any mode for securely transmit data on network and click on send button, this information is necessary for intermediate server for identification of source and destination ip-addresses.

a) Stimulus/Response:
When user selects send button, intermediate server form will get displayed. And selecting appropriate mode that is block or unblock the information received at receiver node.

b) Functional Requirement:
In order transfer the data form source to destination over the network securely.

2) FEATURE:
By choosing one of the modes for securely transferring the data from source to destination, The user selecting the cryptographic puzzle scheme the authentication provided based on expression and shared key algorithm So that only authorized users will have access to information.

a) Stimulus/Response:
When user choose cryptographic puzzles mode and select send button the intermediate server form will get displayed. After clicking unblock mode button, receiver will successfully receive information.

b) Functional Requirement:
To encrypt the data for authentication.

3) FEATURE:
By choosing one of the modes for securely transferring the data from source to destination, the user selecting the Strong hiding commitment scheme the authentication provided based on shared key algorithm. So that only authorized users will have access to information.

a) Stimulus/Response:
When user choose Strong hiding commitment scheme mode and select send button the intermediate server form will get displayed. After clicking unblock mode button, receiver will successfully receive information.

b) Functional Requirement:
To encrypt the data for authentication.

4) FEATURE:
By choosing one of the modes for securely transferring the data from source to destination, the user selecting the all or nothing transmission scheme the authentication provided based on decryption key algorithm So that only authorized users will have access to share information.

a) Stimulus/Response:
When user choose Strong hiding commitment scheme mode and select send button the intermediate server form will get displayed. After clicking unblock mode button, receiver will successfully receive information.

b) Functional Requirement:
To encrypt the data for authentication.

5) FEATURE:
User can view the network traffic signals using the chart.

a) Stimulus/Response:
When user chooses the signal traffic tab on the intermediate server form the signal variations will get displayed. Using this network performance can be evaluated.

b) Functional Requirement:
Analyze the network traffic.

VIII. FUTURE ENHANCEMENT

1) Providing more security at server side by implementing puzzle value at server side securely.

2) Analyze more security algorithms for detecting internal threat attacks.

Our Contributions:

We are checking the feasibility of real-time packet classification for launching selective jamming attacks, under an internal threat model. We are showing that such attacks are relatively easy for nodes or terminal. We are investigating the impact of selective jamming on critical

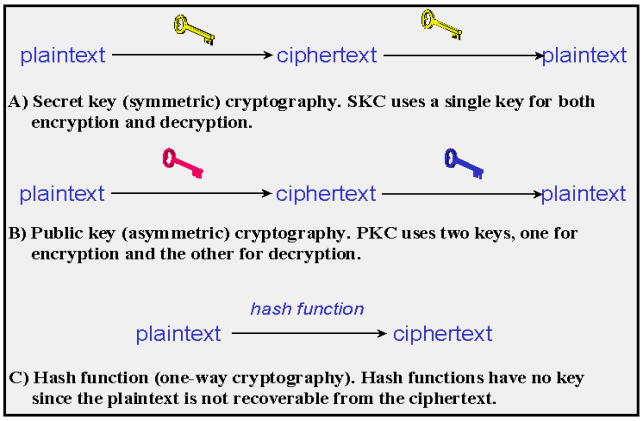
network functions. Our findings indicate that selective jamming attacks lead to DoS with very low effort on behalf of the jammer. To avoid such attacks, we are developing three schemes Cry. Puzzles, SHCS, AONT that prevent classification of transmitted packets in real time. Our schemes rely on the joint consideration of cryptographic mechanisms with PHY-layer attributes. We are providing strong Security to the server.

IX. OBJECTIVES

1) Cryptographic Puzzles:
The three types of algorithms that will be discussed are in Figure 2:
a) Secret Key Cryptography (SKC): Uses a single key for both encryption and decryption.

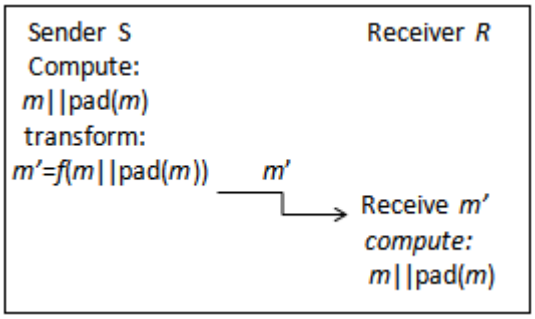
b) Public Key Cryptography (PKC): Uses one key for encryption and another for decryption.

c)Hash Functions: Uses a mathematical transformation to irreversibly "encrypt" information.



2) DES:
(Data Encryption Standard) have a high security level 64 bit related to a small key used for encryption and decryption.It can be easily understood and not depend on the algorithm's confidentiality adaptable and economical be efficient and exportable.

3)All-Or-Nothing Transformations:



4)Impact of Selective Jamming
In this section, we are elaborating the impact of selective jamming attacks on the network performance. the attacker targeted a TCP connection established over a multi-hop network route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process.

5) Selective Jamming at the Transport Layer
For demonstration purpose, transferring a file of a 2 MB file between two users A and B connected via a multi-hop route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/CTS mechanism was enabled. The transmission rate was set to 10 Mbps at each link. The jammer was placed within the proximity of one of the intermediate hops of the TCP connection. Four jamming strategies were considered: (a) selective jamming of cumulative TCP-ACKs, (b) selective jamming of RTS/CTS messages, (c) selective jamming of data packets, and (d) random jamming of any packet.

X. CONCLUSION

In this way, we addressing the problem of selective jamming attacks in networks. We 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.

We showing that the jammer can classify the packets in real time by decoding the first few symbols of an ongoing transmission. We evaluate the impact of selective jamming attacks on network protocols such as TCP and routing. Our findings show that a selective jammer can significantly impact performance with very low effort.

We are developing and survey on three schemes that transform a selective jammer to a random one by preventing real-time packet classification.

XI. REFERENCES

[1] Alejandro Proano and Loukas Lazos "Packet-Hiding Methods for Preventing Selective Jamming Attacks". Presented at IEEE ICC 2010.

[2] G. Sathish Kumar and V. Durgadevi " Providing Network Security by Preventing Selective Jamming Attack".pp 05-09 in Dec-2012.

[3] Bharath J and Rajashekhar S.A "SHCS Technique Defined for Packet Hiding Methods in Wireless Networks".pp in 15-19, March 2013.

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

[5] M. Cagalj, S. Capkun, and J.-P. Hubaux, "Wormhole-Based Anti- Jamming Techniques in Sensor Networks," IEEE

Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114, Jan. 2007.

[6] A. Chan, X. Liu, G. Noubir, and B. Thapa, "Control Channel Jamming: Resilience and Identification of Traitors," Proc. IEEE Int'l Symp. Information Theory (ISIT), 2007.

[7] T. Dempsey, G. Sahin, Y. Morton, and C. Hopper, "Intelligent Sensing and Classification in Ad Hoc Networks: A Case Study," IEEE Aerospace and Electronic Systems Magazine, vol. 24, no. 8, pp. 23-30, Aug. 2009.

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

[9] K. Gaj and P. Chodowiec, "FPGA and ASIC Implementations of AES," Cryptographic Engineering, pp. 235-294, Springer, 2009.

Authors

Katkar Kiran B.
B.E.Computer
University of Pune
Department of Computer Engg.
Govt. College of Engg, & Research,
Awasari (kd),
Tal- Ambegaon, Dist-Pune. India.

Dukare Ajay B.
B.E.Computer
University of Pune
Department of Computer Engg.
Govt. College of Engg, & Research,
Awasari (kd),
Tal- Ambegaon, Dist-Pune. India.

Pawar Monali R.
B.E.Computer
University of Pune
Department of Computer Engg.
Govt. College of Engg, & Research,
Awasari (kd),
Tal- Ambegaon, Dist-Pune.

Darandale Dnyaneshwar R.
B.E.Computer
University of Pune
Department of Computer Engg.
Govt. College of Engg, & Research,
Awasari (kd).Tal- Ambegaon, Dist-Pune.

