ISSN:0975-9646

Packet Hiding Scheme without Packet Loss (PHSPL) for defensive against Jamming Attack

Archana Patil, Prof. S.P.Pingat

Department of Computer Engineering,
Pune university, Pune, India

Abstract— **Normally wireless average greeneries leaves it vulnerable to deliberate intrusion attacks, referred to as jamming. Wireless sensor networks are based on shared medium which makes easy for opponent to conduct radio interference, or jamming, attacks that effectively cause a denial of service on transmitting and receiving functionalities. Typically, jamming has been addressed as a threat model. In this work, we illustrate the impact of selective jamming on the network performance by illustrating various selective attacks in wireless networks. In these attacks, the intruder attacks on the network for a short period of time, selectively directing messages of high importance. To overcome these attacks, we studied existing three schemes& proposed work (PHSPL) that prevents the attacker from attacking the packets. Then we evaluate the security of all schemes.**

Keywords—**PHSPL, DOS attacks, selective jamming, WSN.**

I. Introduction

Wireless networks rely on the sustained availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it susceptible to numerous security threats. Someone with a transceiver can eavesdrop on current transmissions, infuse spurious messages, or jam legitimate ones. While snooping and message addition can be debarred using cryptographic methods, blocking attacks are much harder to counter. They are actually attacked in Dos (denial of service) Attack compared with wireless Attack. It is very easy technique of jamming; this signal is interrupted by receiving of messages by transmitting an uninterrupted jamming signal.

The jamming Attack is considered as external type of attack, in that jamming technique the jammer is not a part of network in this model jamming technique includes continuous or interrupted signals "Always on" Technique has some disadvantages .Firstly the Opponent has increase Amount of Energy to jamming the Frequency of Band. Another type the Continuous present of high Disturbance level creates this type of attack easy to Obtain.

Normally Anti jamming Techniques are mostly depends on spread spectrum communication, or some form of jamming Neglect. Spread spectrum techniques provide Bit level protection by spreading bits According to Secret (pseudo-Noise) PN code. These Techniques can only to protect wireless transmission under the External threat model. Broadcast communication are specially weak under an internal threat model because all receiver must known of the secrets used to protection of the Transmission.

In this paper we are discuss the problem of jamming under an internal Threat model . We are considered this is familiar who is all known of network secrete and implementation Detail of network Protocol at any layer in the network stack. e.g.:- Jammer can target routing request / reply message at the routing layer to secure route Discovery or Destination/Target TCP Response in a TCP session to servery Decrease the output of an End To End flow. Effect of selective jamming on critical network function. To finding to selective jamming attacks lead to a Dos with very low effort on behalf of the jammer. To avoid such attack ,we develop three types of schemes that prevent Classification of transmitted packets in real time .this technique is considered As cryptographic mechanism with physical layer Attributes . we observed that the security of our scheme and show that to achieve strong security properties , with minimum impact of network performance.

II. Problem statement

An Consider the scenario in given figure. Node A and B communicates with wireless or LAN network. With communication range of both A and B there is a jamming Node. When A transfer the packet from m to B, node j classifies m by receiving only the first few Bytes of m .then J corrupts m beyond recovery by interfering with its reception at B. We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J'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.

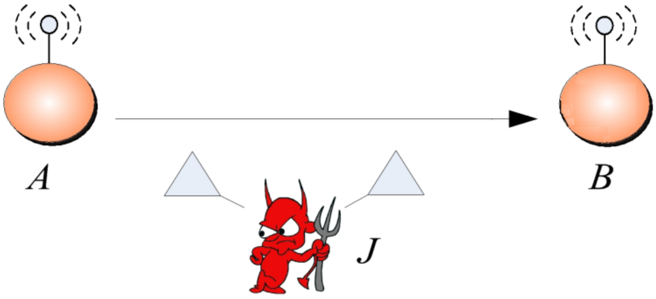

Fig.1. Realization of a selective jamming attack

In this point , we can shows that how the adversary packet can specify packet in real time Once a packet is described, the adversary may choose to jam it depending on his type. Fig.1. at the PHY layer, a packet m is encoded, interleaved, and modulated before it is transmitted over the wireless host. At the receiver, the signal is demodulated, de-interleaved, and decoded, to recover the original packet m. The adversary's ability in classifying a packet m depends on the implementation of the blocks in Fig. 1. The channel encrypting block increasing the original bit sequence m, adding necessary duplication for protecting m against channel errors.

III. Real time classification

All At the Physical 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. Nodes A (Source) and B (receiver) 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.

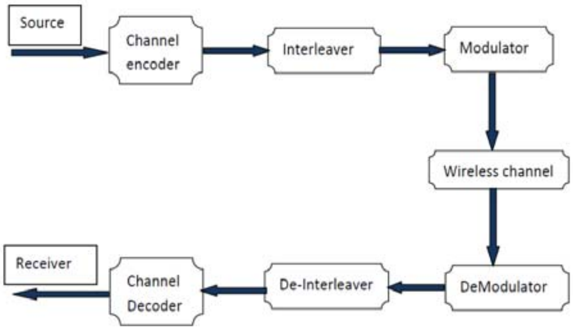

Fig.2. Real Time Packet Classification system diagram

In this section, we show that the problem of real-time packet classification can be mapped to the hiding property of commitment schemes, and propose a packet-hiding scheme based on commitments.

A. A Strong Hiding Commitment Scheme.
B. Cryptographic Puzzle Hiding Scheme.
C. Hiding based on All-Or-Nothing Transformations.

A. **Strong Hiding Commitment Scheme (SHCS)**

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 length s (the length of k is a security parameter). Upon reception of d, any receiver R computes.

B. **Cryptographic Puzzle Hiding Scheme (CPHS)**

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 tp 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.

C. **Hiding based on All-Or- Nothing Transformations (AON-T)**

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 a set of pseudo-messages m = {m1, m2, m3…} is transmitted over the wireless medium

IV. Proposed scheme-packet hiding scheme without packet loss (PHSPL)

In the proposed work, the packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform the 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 a set of pseudo-messages m = {m1, m2, m3,} is transmitted over the wireless link. Recently Rivest motivated by different security concerns arising in the context of block ciphers, introduced an intriguing primitive called the All-Or-Nothing Transform (AONT).

In this scheme we will overcome the Disadvantage of the All-Or-Nothing Transform (AONT). And which also prevents the selective jamming.

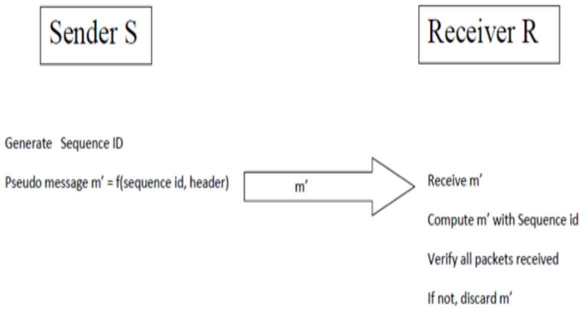
Sender S
Receiver R
Generate Sequence ID
Pseudo message m' = f(sequence id, header)
m'
Receive m'
Compute m' with Sequence id
Verify all packets received
If not, discard m'

Fig.3. Packet hiding scheme without packet loss (PHSPL)

In PHSPL, packets are sending with Header, Sequence ID and host name and the data is send to the selective host. That's why the packet loss is minimum. So the sender and receiver can communicate with each other securely as shown in fig 3. In header of the packet all the information about packet and data. In Header contain Source address, destination address, size of packet and including time stamp. The Sequence ID contains when the packet is encrypted that time the packet is split then send to the another host, because sometime the size of packet is too large then difficult to send so the packet is loss and when the packet is split so send the one by one so the Attacker cannot capture all packet and they don't have sequence id of the packet.

A packet m is send from sender S to receiver R. The packet m is partitioned to set of x input Blocks m= {m1, mx}

Pseudo message are computed as follows;

$m_i' = m_i \oplus Ek'(i)$ for $i=1,2,\ldots\ldots,x$ (1)

$m'_{x+1}= Sqid' \oplus e_1 \oplus e_2 \oplus \ldots\ldots\ldots \oplus e_x$ (2)

Where, $e_i = Ek_0(m'_i \oplus i)$ for $i=1,2,\ldots\ldots\ldots\ldots,x$

k_0 is a fixed publically known encryption key.

The m' is computed again with addition of header, which is as follows

$m' = m'_{x+1} + hdr$ (3)

With reception of all Pseudo messages m is recovered as follows

$m' = Sqid_{\ i} \oplus D_K(Sqid_{\ i+1})$, $i=1,2,\ldots\ldots\ldots\ldots,x$ (4)

Where; $Sqid_{\ i}$= Sequence id for i^{th} .

D_K = Decryption Key

Note that if any m_i' is unknown, any value of $Sqid_{\ i}$ is possible, because the corresponding e_i is not known. Hence, Ek'(i) cannot be recovered for any I, making it feasible to obtain any of $m_{i.}$

V. Conclusions

In this project, the problem of selective jamming attacks in wireless networks. Jammer attacks the importance message because of internal knowledge of network & its secrets. We showed that the jammer can classify transmitted packets in real time by decoding the first few symbols of an ongoing transmission. We evaluated the impact of selective jamming attacks on network. Our findings show that a selective jammer can significantly impact performance with very low effort. We analysed the security of packet hiding schemes and quantified their effectiveness.

We propose the packet hiding scheme without packet loss. In PHSPL, packets are sending with Header, Sequence ID and host name and the data is send to the selective host. That's why the packet loss is minimum. So the sender and receiver can communicate with each other securely. All the information about packet and data is in the header of packet. The PHSPL is more effective over other real time classification methods.

References

[1] P. Tague, M. Li, and R. Poovendran., "*Mitigation of control channel, jamming under node capture attacks*". IEEE Transactions on Computing, 8(9):1221–1234, 2009.

[2] T . X. Brown, J. E. James, and A. Sethi." *Jamming and sensing of Encrypted wireless ad hoc networks*". In Proceedings of MobiHoc, pages 120–130, 2006.

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

[4] O Goldreich. *Foundations of cryptography: Basic applications*, Cambrige University press.

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

[6] T.dempsey,G.Sahin,Y Morton, and C.Hopper. *Intelligent sensing and classification in ad hoc networks: a case study Aerospace and Electronic Systems* Magazine,IEEE, 24(8)23-30 august 2009 (2002).

[7] 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

[8] B. Greenstein, D. Mccoy, J. Pang, T. Kohno, S. Seshan, and D. Wetherall "*Improving wireless privacy with an identifier-free link layer protocol*". In Proceedings of MobiSys, 2008.

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

[10] Y.Desmedt, Broadcast anti-jamming system,. Computer Networks 35(2-3):223–236, February 2001.