International Journal of Engineering Innovation & Research
Volume 3, Issue 3, ISSN: 2277 – 5668

Cryptographic Techniques for Avoiding Discriminating Congestion Attacks in Wireless Networks

Basamma Koti Alias Gadagi
IV Semester, M.Tech. Deptt. of CSE,
M. S. Engineering College, Bangalore, Karnataka, India
Email: bn.koti@gmail.com

Mrs. Aruna M. G.
Associate Professor, Deptt. of CSE,
M.S. Engineering College, Bangalore Karnataka, India
Email: aruna_mg@yahoo.com

Abstract **– Wireless sensor networks are vulnerable to various interference security threats generally referred to as congestion or jamming attacks. The intentional interference with wireless transmissions will be used for the generation of Denial-of-Service attacks on wireless networks. Adversaries with internal knowledge of protocol specification and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. This work addresses the jamming attacks under an internal threat model, where the adversary is active for a short period of time and selectively targeting the messages of high importance. Discriminating jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, this work proposes four efficient packet-hiding schemes that prevent real time packet classification by combining cryptographic primitives with physical-layer attributes. Random key distribution method used to generate hash bytes provides a more secured packet transmission approach in wireless networks.**

Keywords **– Discriminating Jamming, Denial-of-Service, Packet Classification, Wireless Networks.**

I. INTRODUCTION

Wireless networks are the interconnection of participating nodes to provide an uninterrupted availability of wireless medium. However, the networks are attacked by various security threats due to the open nature of the medium. Adversaries can eavesdrop on wireless medium, inject spurious messages or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to detect and counter. They have been shown to actualize severe Denial-of-Service attacks against wireless networks [1]. Typically jamming attacks have been addressed under an external threat model, in which jammer is not part of the network. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect message transmissions. Hence, compromise of a single receiver is sufficient to reveal relevant cryptographic information. The objective of our work is to address the problem of jamming under an internal threat model where the jammer can exploit his internal knowledge to launch discriminating jamming attacks targeting the "high importance" messages. For example targeting route request/route reply messages at the routing layer to prevent route discovery or targeting TCP acknowledgements to degrade TCP sessions.

To launch discriminating 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[2] or by decoding packets on the fly [4]. 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. Discriminating jamming requires an intimate knowledge of the physical layer and the specifics of upper layers.

We investigate the feasibility of real-time packet classification for launching selective jamming attacks, under an internal threat model. These attacks are relatively easy to actualize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes. Congestion attacks lead to a DoS with very low effort on behalf of the jammer. We proposed four schemes that prevent that prevent real time packet classification of transmitted packets.

II. RELATED WORK

A. Problem Statement

A is communicating with B via wireless link as depicted in Fig. 1. Within the communication range of both A and B, jamming node J is present. 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. We address the problem of 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.

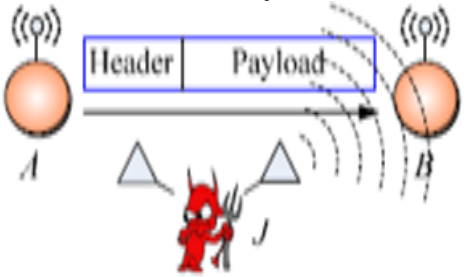

Fig.1. Realization of a Selective Congestion Attack

B. Network and Communication Model

The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly or

indirectly. Nodes communicate both in unicast mode or broadcast mode. Communications can be either encrypted or unencrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre-shared pairwise keys or asymmetric cryptography.

Transmitted packets have the generic format depicted in Fig.2. The preamble is used for synchronizing the sampling process at the receiver. The physical layer header contains information regarding the length of the frame and transmission rate. The MAC header determines the MAC protocol version, the source and destination address, sequence numbers plus some additional fields. Frame body contains an ARP packet or an IP datagram. MAC frame is protected by a cyclic redundancy check(CRC). At the PHY layer, a trailer may be appended for synchronizing the sender and receiver.

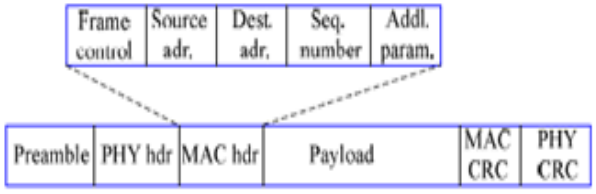

Fig.2. A Generic Frame Format.

C. Real Time Packet Classification

Consider the generic communication system depicted in Fig. 3. 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.

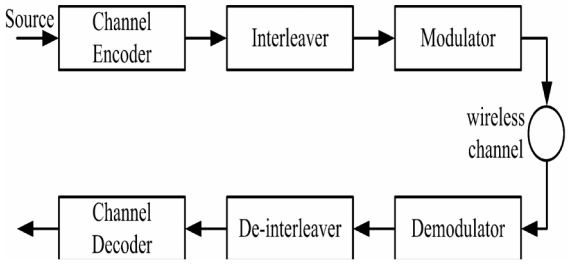

Fig.3. A Generic Communication System.

D. Adversary Model

We assumed that the adversary exists within the communication range of source and sink. He is in control of communication medium and can jam messages at any part of the network of his choosing. The adversary can operate in full duplex mode. 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. Adversary can selectively jam a discriminated number of bits and irrecoverably corrupt a transmitted packet by jamming the last symbol. A jammer equipped with a single half-duplex transceiver is sufficient to classify and jam transmitted packets. Furthermore, the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic for network architectures such as mobile ad-hoc, mesh, cognitive radio, and wireless sensor networks, where network devices may operate unattended, thus being vulnerable to physical compromise.

III. PROPOSED WORK

To mitigate real time packet classification in wireless sensor networks and for avoiding discriminating jamming attacks, we proposed four cryptographic techniques. The objective of these techniques is to transform a discriminate jammer to a random one. Fig. 4 depicts the system architecture. It has three modules such as client, intermediate node and server. Thefour techniquesare developed for preventing discriminating congestion attacks by combining cryptographic primitives with physical layer attributes. These techniques include Strong Hiding Commitment Scheme (SHCS), Cryptographic Puzzle Hiding Scheme (CPHS), AONT-based Hiding Scheme (AONT) and Random Key Distribution Scheme (MD5).

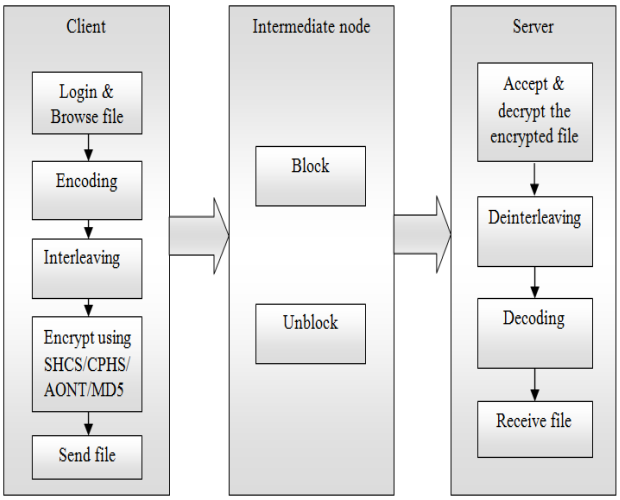

Fig.4. System Architecture

The client has to browse a file (*.txt, *.doc, *.docx) for the secured transmission. Then performs channel encoding followed by interleaving where these two operations provide a security within a packet. Next encrypts the packet using either Strong Hiding Commitment Scheme (SHCS) or Cryptographic Puzzle Hiding Scheme (CPHS) or AONT Scheme (AONT) or Random Key Distibution Method (MD5) and broadcasts the packet. Later the packet is transmitted through intermediate nodes via Block/Unblock mode and is forwarded to the server. Server accepts the encrypted data. Then it decrypts it by using key, de-interleaves, decodes and finally obtains the file content in the original format sent by the sender.

Block mode in the intermediate node is the one where the packets are attacked by the adversary. Unblock mode is the normal data transmission mode. We proposed the cryptographic techniques, using which the packets attacked by the adversary also sent successfully to the receiver.

International Journal of Engineering Innovation & Research
Volume 3, Issue 3, ISSN: 2277 – 5668

A. *Strong Hiding Commitment Scheme (SHCS)*

Commitment schemes are cryptographic primitives that allow an entity A, to commit to a value m, to an entity V, while keeping m hidden [6].

SHCS is based on symmetric cryptography. The objective of this scheme is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. Here the commitment function $E_k()$is the symmetric encryption algorithm like DES or AES.

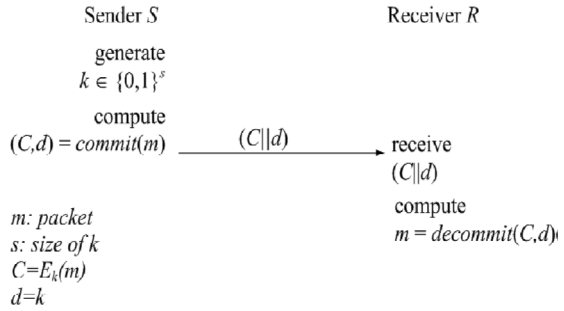

Fig.5. Strong Hiding Commitment Scheme

Consider that sender S has a packet m for R. First, S constructs (C, d) =Commit (m), where, $C=E_k(\pi_1(m))$, d=k. Here the commitment function E_k is a symmetric encryption algorithm. π_1 is a publicly known permutation and k € {0,1}s is a randomly selected key of some desired key length s. The sender broadcasts (C || d), where || denotes the concatenation operation. Upon reception of d, any receiver R computes $m=\pi_1\text{-}1(D_k(c))$ as shown in Fig. 5.

SHCS scheme requires the joint consideration of the MAC and PHY layers. To achieve the strong hiding property a sublayer called the "hiding sublayer" is inserted between the MAC and the PHY layer. The functions of the sublayer are shown in Fig. 6.

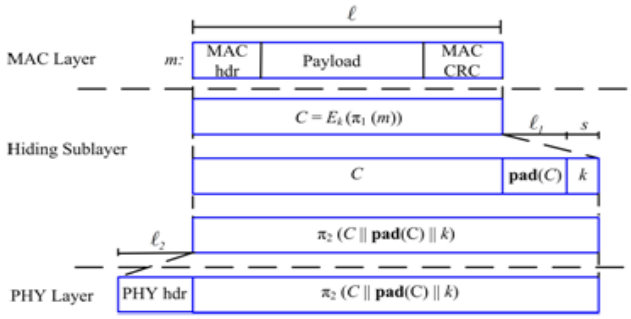

Fig.6. Processing at the Hiding Sub Layer.

B. *Cryptographic Puzzle Hiding Scheme(CPHS)*

CPHS force the recipient of the puzzle to execute a set of computations before he is able to extract a secret of interest. The time required for obtaining the solution depends on its hardness and the computational ability of the solver. Here the benefit is the security does not rely on the PHY layer parameters.

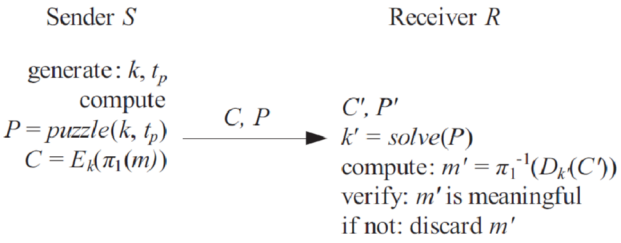

Fig.7. Cryptographic Puzzle Hiding Scheme

CPHS is used to temporarily hide transmitted packets. Here the packet m is encrypted with a randomly selected symmetric key k of a desirable length s as depicted in Fig.7. The key is blinded using a cryptographic puzzle and sent to the receiver. The puzzle carrying k cannot be solved before the transmission of encrypted version of m is completed and the puzzle is received. Hence, the adversary cannot classify m for the purpose of selective jamming.

C. *All-or-Nothing Transformations (AONT)*

Packets are preprocessed by AONT before the transmission. The jammer can-not perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. The message m is divided into number of packets. Using these packets the pseudo messages are created and sent to the receiver. The jammer cannot perform packet classification until all the 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 = {m_1, m_2, m_3….}, which serve as an input to the set of pseudo-messages m^1={m_1^1, m_2^1, m_3^1,…..} is transmitted over the wireless medium. The transformation is based on bijection and it is computationally infeasible to obtain any part of the original plain text, if one of the pseudo-messages is Unknown.The algorithm for AONT is shown in the Fig.8.

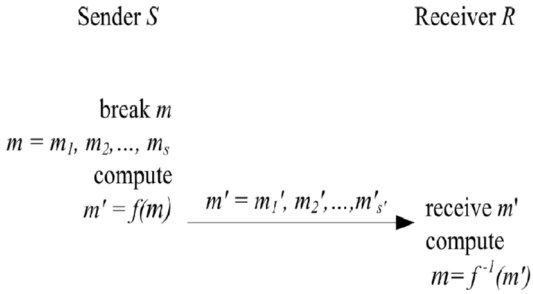

Fig.8. AONT-based hiding scheme.

When a plaintext is pre-processed by an AONT before encryption, all ciphertext 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 ciphertext blocks, without any change on the size of the secret key.

D. *Random Key Generation Method (MD5)*

Message Digest (MD) algorithms, also called as Hash algorithms; generate a unique message digest for an arbitrary message. When a password is encrypted by a

hash algorithm the resultant is called hashed password. In a server client based communication systems passwords of clients are hashed by MD5 and passed to the server for authentication. This type of transmissions are always a subject of interception by the hackers. These hashed passwords are passed through the internet as a data packet. TCP header is a most common part of the data packet. In a TCP header there are six reserved bits which remain always unused. The paper proposed a new approach to enhance the security of hashed passwords by using the six reserved bits of a TCP header. Here we encrypt the hashed password by a random key using simple mathematical function. The information needed to decrypt the encrypted hashed password is carried by the six bits of TCP header.

IV. SNAPSHOTS

This part provides the snapshots of results obtained for the implementation of Cryptographic Techniques for Avoiding Discriminating Congestion Attacks in Wireless networks.

A. Client Login Page

Fig.9 shows the login page. Client needs to enter the name and password that is registered in the database. New user can register his details to get new account for the secured data transmission.

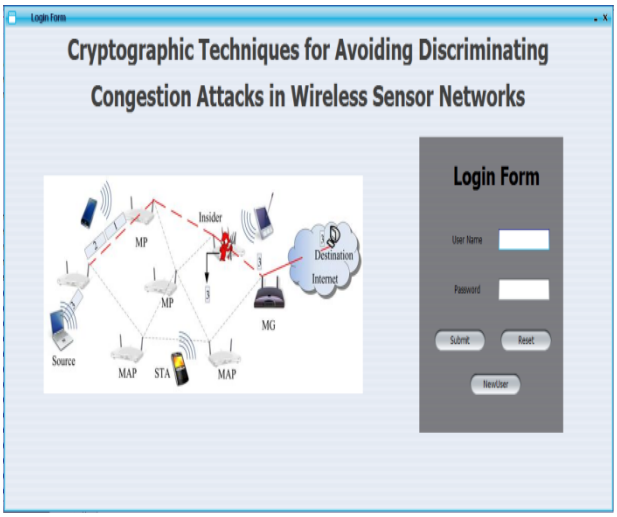

Fig.9. Login Page

B. Intermediate Node

Fig. 10 shows the intermediate node page. It provides packet details after the data transmission. It contains 2 modes called block and unblock. Block mode is the one, where packet is attacked by the intruder. Unblock mode is the unaffected mode.

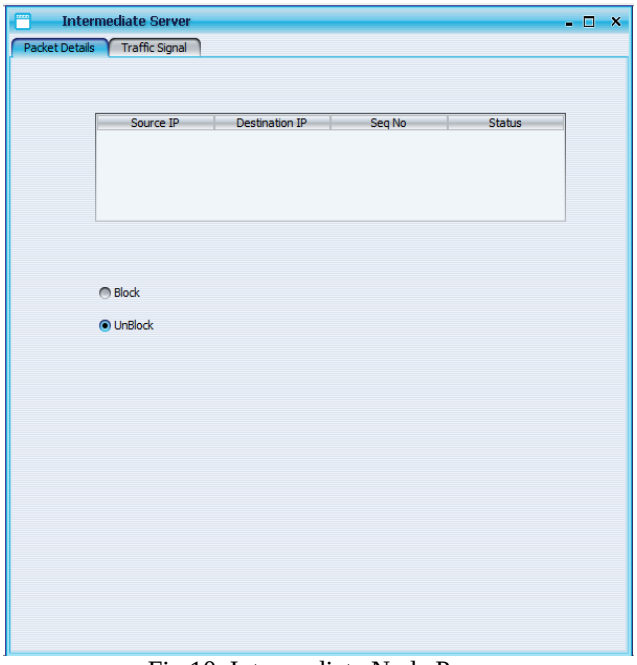

Fig.10. Intermediate Node Page

C. Client Page of Encrypting Data

Client needs to select a text file, then encode the data, interleave and encrypt using one of the four cryptographic techniques and send to the receiver as shown in Fig.11.

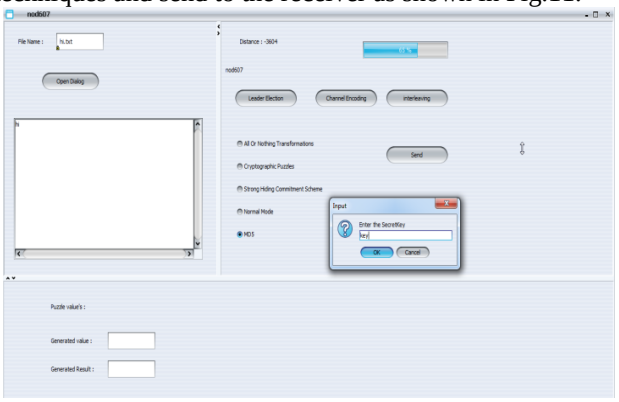

Fig.11. Client Page

D. Encrypting and Decrypting Data

The Fig.12 shows Random Key Distribution scheme's encryption and decryption process. Pop up window appears informing the leader node (sender node). Sender needs to enter secret key. The MD5 scheme will generate a hashed value using the secret key. At the receiver side, receiver needs to enter the same hash value, which he will get in his registered mail id. To get the data.

Fig.12.Encryption and Decryption

E. Data Encoding

The Fig. 13 shows the data encoding process. First the text data will be converted to ASCII value then to binary values.

```
**********************Channel Encoding Started***************
5
Int Value : [0] = 103
Int Value : [1] = 111
Int Value : [2] = 111
Int Value : [3] = 100
Int Value : [4] = 0
1100111
1101111
1101111
1100100
0
1 1 0 0 1 1 1
1 1 0 1 1 1 1
1 1 0 1 1 1 1
1 1 0 0 1 0 0
0
111 111 000 000 111 111 111
111 111 000 111 111 111 111
111 111 000 111 111 111 111
111 111 000 000 111 000 000
000
11111100000011111111
11111100011111111111
11111100011111111111
11111100000011000000
000

**********************Channel Encoding Completed***************
```

Fig.13. Data Encoding

F. Data Interleaving

The Fig.14 shows the data interleaving process. The encoded data is shuffled and split to form packets. Then the data is sent for encryption.

```
**********************Interleaving Started**************
1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 1 1 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 0 0 0 1 1 1 1 1 1 1 1 1 1 1
1 1 1 1 1 1 0 0 0 0 0 0 1 1 1 0 0 0 0 0
0 0 0
1 1 0 0   0 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1
1 1 1 1 0 1 0 1 1 1 1 1 1 0 1 1 1 1 1 1 1
1 1 1 1 0   0 1 1 1 1 1 1 0 1 1 1 1 1 1 1
1 1 0 0 0 0 0 0 1 1 1 0 1 0 0 1 0 0 1 0 1

Packet [0] = 1100 0011111101111111
Packet [1] = 111101011111101111111
Packet [2] = 11110 011111101111111
Packet [3] = 110000001110100100101
Packet [4] =

**********************Interleaving Completed**************
```

Fig.14. Data Interleaving

V. CONCLUSION

The work addresses the problem of discriminating congestion attacks in wireless networks by considering an internal adversary model in which 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 ongoing transmission so that the packet cannot be recovered at the receiver. We developed four techniques for the prevention of discriminating jamming attacks. These schemes transform a selective jammer to a random one by preventing real-time packet classification.

The schemes combine cryptographic primitives such as Strong Hiding Commitment Scheme (SHCS), Cryptographic Puzzle Hiding Scheme (CPHS), AONT-based Hiding Scheme (AONT) and Random Key Distribution Scheme (MD5).The security of these schemes are quantified with their computational and communication overhead.

As of now the application is working fine for symmetric and brute force algorithms. They may be overridden by new and efficient algorithms if needed. The project work can be made functional to transmit even .jpg, .ppt or .pdf and other such file formats.

REFERENCES

[1] L. Lazos, S. Liu, and M. Krunz. Mitigating control-channeljamming attacks in multi-channel ad hoc networks. In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 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] A. Chan, X. Liu, G. Noubir, and B. Thapa. Control channel jamming: Resilience and identification of traitors. In Proceedings of ISIT, 2007.

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

[5] O. Goldreich. Foundations of cryptography, Basic applications. Cambridge University Press, 2004.

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

AUTHOR'S PROFILE

Basamma Koti Alias Gadagi
is currently a final year student of M.S. Engineering College, Bangalore, Karnataka. She is doing her masters in Computer Science and Engineering. She received her bachelor's degree in Information Science from BEC, Bagalkot. Her areas of interest are Wireless Sensor Networks and Network Security.

Mrs. Aruna M. G.
received her M. Tech in Computer Science and Engineering from Dr. MGR University in 2006. She received her bachelor's degree in Computer Science and Engineering from Bangalore University in 2001. She is currently doing her Ph. D in Computer Networks from VTU. Her areas of research include Network Security and Cloud Computing.