A Novel Method for Averting Jamming Invasion in Wireless Network with Packet Hiding Methods

Mamatha B[#1], Dr. Shubhangi D.C[#2], Shridevi Soma[#3].

[#1]P.G.Student, Department of Computer Science & Engineering, VTU RO PG Centre, Gulbarga, Karnataka, India.
[#2]Professor & Course Co-ordinator ., Department of Computer Science & Engineering, VTU RO PG Centre, Gulbarga, Karnataka, India.
[#3]Associate Professor, Department of Computer Science & Engineering, PDACE, Gulbarga, Karnataka, India.

ABSTRACT

Wireless medium is open in its nature and hence it is obvious to have intentional interference attacks that are referred as jamming. It works by denying service to approved users as genuine traffic is jammed by the overwhelming frequencies of illegal traffic. Typically external threat models address jamming. However here we consider the adversaries with interior knowledge of protocol specifications and network secrets that can initiate low-effort jamming attacks which are difficult to detect and respond. Thus we address the problem of jamming attacks internally in wireless networks. During such attacks, the opponent remains active only for a small period of time, selectively targeting messages of high importance. We investigate the feasibility of real time packet classification for introduction selective jamming attacks on physical layer. To mitigate these attacks and impact of attacks on network functions we develop three schemes that prevent classification of transmitted packets in real time by combining cryptographic mechanisms with physical layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), and All-Or-Nothing Transformation Hiding Schemes (AONTHS).Cryptographic hash function using MD5 message digest applied to the above schemes to give more secured packet transmission in wireless networks.

Key word: Denial of Service, MD5, Selective Jamming, Wireless Network, AONT, Spread Spectrum, Packet Classification.

1. INTRODUCTION

A wireless sensor network and Wireless telecommunications networks are commonly implemented and administered using radio communication. This implementation takes place at the physical layer of OSI model network structure.

These networks are open in their nature and are vulnerable to various securities threats and rely on continuous availability of medium for transmission and hence are vulnerable to intentional interference attacks, normally referred to as jamming.

This intentional interference attacks acts as a platform to launch denial of service attacks. These attacks make resources busy to planned users. Jamming is one of the many attacks used to compromise the wireless environment. These are complex attacks that are much harder to counter and are typically considered under external threat model. Jamming makes itself known at the physical layer of the network, more usually known as the MAC layer. Here consider the possibility of real time packet classification for launching selective jamming attacks on physical layer. Thus we consider the internal threat model with protocol specification and network secrets to provide security. Here we address the problem of selective jamming attacks where opposition is active only for a short period of time, selectively targeting messages of high importance.

To mitigate these attacks and impact of attacks on network functions, three schemes are developed that prevent classification of transmitted packets in real time by combining cryptographic mechanisms with physical layer attributes. They are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), and All-Or-Nothing Transformation Hiding Schemes (AONTSHS). Cryptographic hash function using MD5 message digest applied to the above schemes to give more secured packet transmission in wireless networks.

This paper is organized as follows, Section 2 explains the concept of related work for packet hiding methods for preventing the selective jamming attacks. Section 3 dictates proposed system. In Section 4 experimental results are discussed. Finally Section 5 contains conclusion and future work.

2. RELATED WORK

Continuous jamming has been used as a denial-of-service (DoS) attack against voice communication since the 1940s [11]. Recently, several alternative jamming strategies have been established [10]. Xu et. al. Categorized jammers into four models, (a) a constant jammer that continuously emits noise, (b) a deceptive jammer that continuously broadcasts fabricated messages or replays old ones, (c) a random jammer that alternates between periods of continuous jamming and inactivity, and (d) a reactive jammer who jams only when transmission activity is detected. Intelligent attacks which target the transmission of specific packets were presented in [8]. Thuente considered an attacker who infers important packet transmissions based on timing information at the MAC layer. Law et. al. considered(a) (b).

Selective jamming attacks in multi-hop wireless networks, where future transmissions at one hop were conditional from prior transmissions in other hops. However, in both [8], real-time packet classification was considered outside the capabilities of the adversary. Selectivity was achieved via inference from the control messages already transmitted. Channel-selective jamming attacks were considered in [4]. It was shown that targeting the control channel reduces the required power for performing a DoS attack by several orders of size. To protect control

channel traffic, control information was fake in multiple channels. The "locations" of the channels where control traffic was broadcasted at any given time, was cryptographically protected. In [12], proposed a randomized frequency hopping algorithm, to protect the control channel inside jammers. Finally, Popper et. al. proposed a frequency hopping anti-jamming technique that does not want the sharing of a secret hopping sequence, between the communicating parties [13].

Selective jamming problem has been addressed under various threat models. The impact of external selective jammers targeting different control packets at the MAC layer is studied in the paper [8] by author Thuente. Selective jamming attack is based on protocol semantics, where they considered several packet identifiers for enciphered packets such as packet size, signal sensing and timing information of different protocols. Unification of packet characteristics like minimum length and the inter packet timing was used in order to prevent selectivity. In [1], the author's attempts to make use of protocols at various layers to get three advantages- targeted jamming, jamming gain, and reduced probability of detection. In targeted jamming attack, it may jam particular nodes, flows or links. Here the adversary may be interested in specific parts of the network and attacking those regions can lead to further jamming gains, where as in reduced probability of detection, the sufferer network may not be aware of jamming attack counter measures. Selective jamming attacks have been experimentally implemented using the software defined radio engines [9]. USRP2-based jamming platform called RFReact was implemented in [9] that enable selective and reactive jamming. In this paper develop four schemes that prevent jamming attacks. They are Message digest algorithms along with SHCS, CPHS and AONT.

3. PROPOSED SYSTEM

It is usual anti-jamming techniques broadly on spread-spectrum connections, or else some form of jamming avoidance as per some example is spatial retreats or slow frequency hopping. A spread spectrum technique gives bit-level of security by distribution the bits according to a secret pseudo noise code as called only the communicating parties. This type of methods can only protect in wireless network or transmission in the outside or external threat model, possible permission of secrets suitable for the nodes compromise with neutralizes the gains of SS. Here the connection are shown for the mainly in vulnerable or danger under the internal threat model, why because all the particular user wants receive, they must aware of the secrete use for the protect transmission, therefore, the cooperation of an only receiver is enough to expose relevant cryptographic information.

In this model, jamming strategies contains the continuous transmission of high power intrusion signals, still adopting an "always-on" strategy are shown some disadvantages below

- First, the opponents use an important amount of energy to jam frequency bands of attention.
- Second, continuous occurrence of jammer shows the high interference levels make this type of attack easy to detect.
- Broadcast connections are mainly vulnerable to the internal threat model. Because all intentional receivers must be aware of the secrets that is use for protect transmissions.
- Someone with a transceiver can listen in on wireless transmissions, insert false messages, or jam valid ones.

- In the wireless network it is very danger ,the intentional interference attacks classically referred to as jamming
- Therefore, the compromise of a single receiver is enough to expose relevant cryptographic information.
- Hence, cooperate of a single receiver is sufficient to reveal relevant cryptographic information.

In this work, we addressed the difficulty or problem of jamming under an internal threat model. Here considering the difficult opponent who is aware of network secret and shows the details of the network protocols at any layer in the network stack. The opponent exploits his internal knowledge for beginning selective jamming attacks in which particular messages of "high importance" are under attack as per example, a jammer can target route-request/route-reply messages at the routing layer to stop route discovery, or targets acknowledgments in a TCP session to severely degrade the throughput of an end-to end flow. As per the Fig. 1 shows below is the basic architecture of the proposed system.

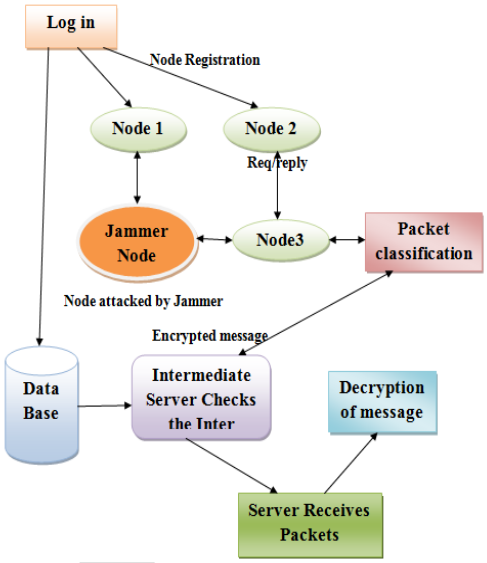

Fig.1: Basic Architecture

Some of the advantages of the proposed system are

- Provides security to the internal threat model considering the specifications of protocols and secrets network security.
- Security is provided by considering the cryptographic mechanisms with physical layer attributes. Thus strong security properties are achieved.
- The selective jamming attacks on protocols TCP and routing protocols significantly impact performance with low effort.

A. Real Time Packet Classification

In the real time packet classification express how the opponent can classify the packets in the real time, by the packet transmission is done, once packet is classified the opponent may choose to jam it depending on its approach. Consider the general message system represent in Fig 2. At

the physical layer, a sender send the packet m to the channel encoded, interleaved, and modulated before it is transmit over the wireless channel. At the receiver side, the signal is demodulated, de interleaved, and decoded, to recover the original packet m.

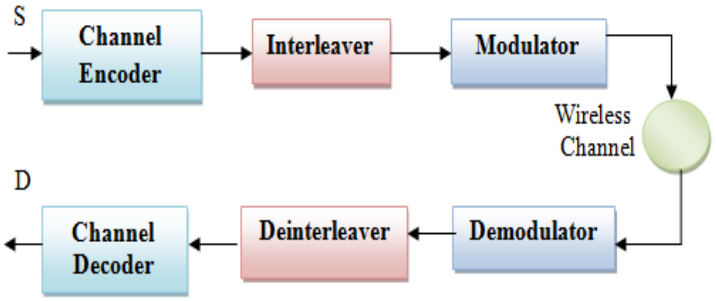

Fig. 2: A generic communication system diagram.

If we are using a hiding scheme for the encryption key should be remain secrete, the still portion of a transmitted packet might be potentially guided to packet classification, since it is for computationally-capable encryption technique are block encryption, the encryption of the prefix plaintext with the similar key given in a static cipher text prefix, therefore, an opponent who is aware of the essential protocol specifics such as structure of the frame, they can use the static cipher text section of a transmitted packet to classify it.

B. A Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS) shows that SHCS is based on symmetric cryptography. Their main goal is to satisfy the strong hiding scheme as keeping the addition overhead to a minimum.

A commitment scheme allows an entity "S" has sender, to commit to a chosen value, to another entity "V" while keeping that value hidden to others. Commitment scheme must satisfy the following two properties:

- Binding**:** Deliver the committed value to the receiver end, here the sender cannot alter the value once it is committed
- Hiding**:** The receiver cannot see the message until he gets the secret key, after receiving the key receiver verifies that it is indeed the message to which the sender is committed. Here the role of the committer is occupied by the sender or transmitting node, whereas role of the verifier is implicated by any receiver including the attacker. Consider the Fig 3 shows that sender S has a packet "m" for the transmission for receiver R. First, before transmission S constructs the following

(C,d) = commit (m), where $C= E_k (\pi_1(m))$, $d=k$

Where '$E_k()$' the commitment function is an symmetric encryption algorithm for example DSA or RSA algorithm, 'π'_1 is a publicly known permutation and $k€\{0,1\}^s$ is a randomly selected key. At the receiver end, upon receiving 'd' the receiver 'R' computes $m = \pi_1^{-1}(D_k(C))$, where 'π_1^{-1}' is the inverse permutation of 'π'_1 and also it verifies the signature which is attached to the packets.

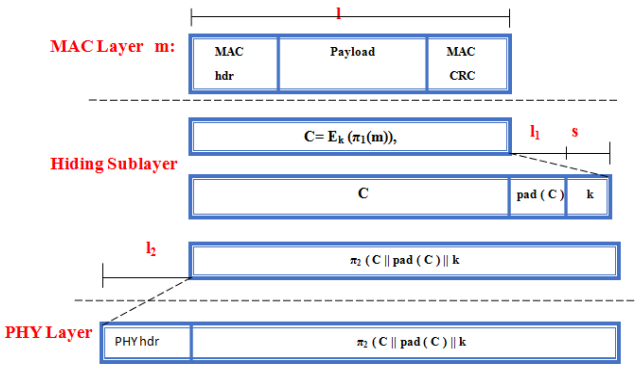

Fig.3: Packet Format

C. Cryptographic Puzzle Hiding Scheme

Cryptographic puzzles is based on the packet hiding scheme, the main motivation behind such type of puzzles is to force the receiver of a puzzle perform a pre-defined set of calculation before he is able to take out a secret of interest.

This work present a packet hiding scheme based on cryptographic puzzles, 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 physical layer parameter; In the Fig 4 shows a sender S has a packet m for transmission. The sender selects a random key k€$\{0,1\}^s$ of a desired length. S generates a puzzle (k,t_p), where puzzle () denotes the puzzle generator function, and t_p 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 Ɲ 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.

Sender S		Receiver R
Generate:k,t_p		
Compute		
	C, P	C', P'
$P=puzzle\ (k,t_p) \rightarrow$		k'=solve(p)
$C=E_k(\pi_{1(m)})$		compute:$m'=\pi_1^{-1}(D_k(C'))$
		Verify: m' is meaningful
		If not discard m'

Fig. 4: The cryptographic puzzle-based hiding scheme.

D. All-Or-Nothing Transformations based on Hiding

All-or-Nothing Transforms (AONTs) were introduced by Rivets in 1997, to slow down brute force attacks against block encryption algorithms. The AONT provide as a publicly identified and entirely invertible preprocessing step to the plaintext, earlier it is passed to an common block encryption algorithm .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. Packets are preprocessed by an AONT before transmission to this still it's remains unencrypted the below Fig 5 shows below.

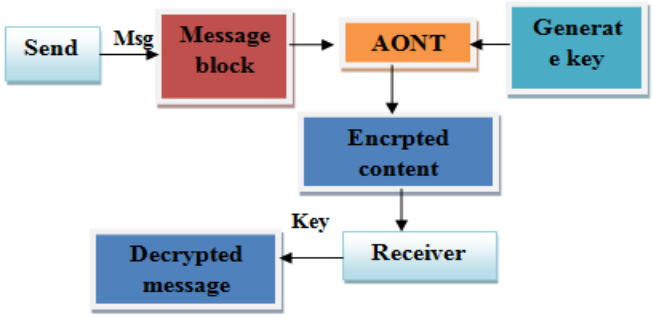

Fig. 5: AONT- based packet hiding method

Packet 'm' is split into a set of 'x' input blocks m = {m1, m2, m3….}, which give out as input to an AONT here, $f:\{IF_u\}^x \rightarrow \{IF_u\}^{x'}$, here '$IF_u$' denotes the alphabet of blocks, 'm_i' and 'x_i' are the output of the pseudo-messages. The set of pseudo-messages m = {m1, m2, m3…} is transmitted over the wireless network. Here we used to have a jammer who tries to decrypt the packet on the fly, when the packets are been transmitted by an ordinary mode they can be easily decrypted by intentional interference attack but when we use the cryptographic primitives it can't be decrypted on the fly from source to destination. So in this paper developed the four schemes for the secure data transmission on the vulnerable medium.

E. MD5 Algorithm

The MD5 message-digest algorithm is a widely used cryptographic hash function producing a 128-bit (16-byte) hash value, typically expressed in text format as a 32 digit hexadecimal number. MD5 has been utilized in a wide variety of cryptographic applications, and is also commonly used to verify data integrity. MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function.

The below Fig 6. illustrate the MD5 Algorithm Structure, When a password is encrypted by a hash algorithm the resultant is called hashed password. This type of transmission is 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 remains always unused. In this project we propose 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 numerical function. The information needed to decrypt the encrypted hashed password is carried by the six bits of TCP header.

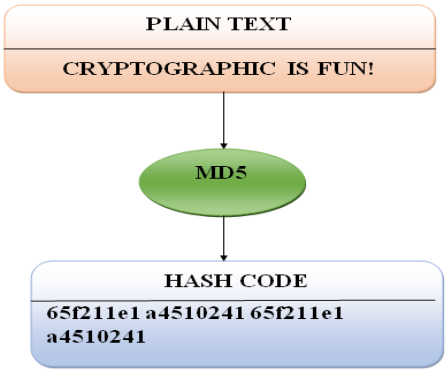

Fig. 6: MD5 Algorithm Structure

The MD5 algorithm get as input message of random length and generate as output 128-bit (four 32-bit words).the message processed in 512-bit (sixteen 32-bit words) blocks. The MD5 algorithm is planned to be somewhat fast on 32-bit machines. In count, the MD5 algorithm doesn't need any huge substitution tables. The algorithm is able to exist coded quite compactly.

4. EXPERIMANTAL RESULTS

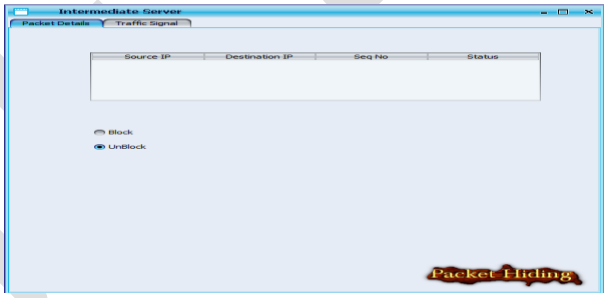

Fig 7: Intermediate server

The fig 6 shows intermediate server, there are two parts in the figure, one is packet details and other one is traffic signal. In the packet details, the source IP address, destination IP address, sequence number and status is present. And there are status information namely block mode and unblock mode.

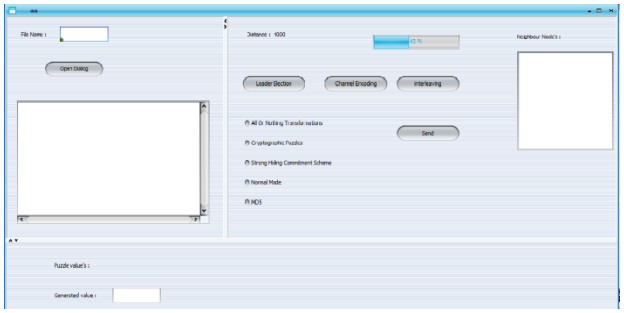

Fig 8: Client Node

The fig 7 shows the Client node, the procedure is as follows, first select the file to be transmitted in the wireless channel by browsing the text file, next we get on to the leader node., after that select the algorithms next it will take the channel encoding and interleaving will takes place, lastly send button for sending the data or file transferring to server side.

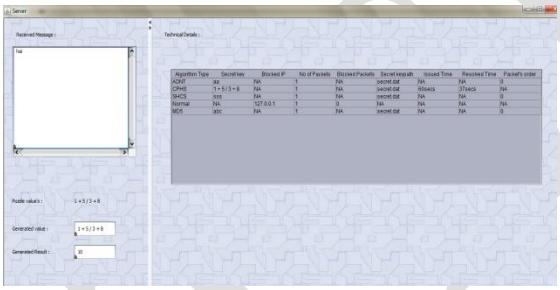

Fig 9: Server Node with data

The fig 8 shows the final step after all the algorithms have been selected. Here, four algorithms are being used for secure transmission and one for normal mode transmission without any security measures during transmissions. The AONT, CPHS, SHCS and MD5 are the four algorithms used for secure transmission. In the AONT and SHCS algorithms, one has to give secret key while sending the file as well as receiving the file. In the CPHS algorithm, at the sender side reference time in seconds will be indicated and at the receiver side the puzzle has to be solved within the specified time at the sender time. In the proposed algorithm i.e. MD5 algorithm, the secret key will be asked at the client side and at the server side the receiver will generate the hash code and this hash code will be mailed to the specified mail ID.

5. CONCLUSION

The problem of choosy blocking attacks in wireless networks has been addressed an internal opponent model in which the jammer is part of the network under attack, thus being conscious of the protocol specifications and common network secrets. It 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 particular blocking attacks on network etiquettes such as TCP and routing. Proposed result in this work shows that particular jammers can significantly collision performance with very low effort, three schemes are developed that transform a particular jammer to a random one by preventing real-time packet classification. There schemes combine cryptographic primitives such as commitment schemes, cryptographic puzzles, all-or-nothing

transformations (AONTs) with physical layer characteristics and also a message digest algorithm (MD5) is developed for secure transfer .

ACKNOWLEDGMENT

The authors would like to thank a great support of VTU University Belgaum and VTU RO PG Centre, Gulbarga, Karnataka, India. Under take this work successfully.

REFERENCE

[1] T. X. Brown, J. E. James, and A. Sethi. Blocking and sensing of encrypted wireless ad hoc networks. In Proceedings of MobiHoc, pages 120–130, 2006.

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

[4] Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010.

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

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

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

[8] D. Thuente and. Acharya. Intelligent blocking in wireless networks with applications to 802.11 b and other networks. In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.

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

[10] 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.

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

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

[13] C. Po¨pper, M. Strasser, and S. C˘ apkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.