IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
ISO 3297:2007 Certified
Vol. 6, Issue 1, January 2017

Implementation of SHCS and AONT Methods for Hiding Packets in Wireless Networks

Shaik Mahammad Rasheed[1], M. Giridhar Singh[2]

Assistant Professor, Dept of CSE, Dr. Abdul Haq Urdu University, Kurnool, Andhra Pradesh[1, 2]

Abstract: The open nature of wireless medium makes it vulnerable to intentional interference attacks, which are typically referred to as jamming. This intentional interference with wireless transmissions can be used as a launching pad for mounting denial of service attacks in wireless networks. Usually, the interference has been addressed in one form of external threat. However, adversaries with inner knowledge of protocol specifications and network secrets can launch low-effort jamming attacks that are difficult to detect and counter. In this paper the problem of selective jamming attacks in wireless networks are addressed. In these attacks, the adversary is active only during a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective blockade in terms of degradation of network performance and adversary effort by presenting two case studies; a selective attack on TCP and one in the routing. We show that selective jamming attacks can be initiated by performing packet classification in real time at the physical layer. To mitigate these attacks, two schemes which prevent the classification of packets in real time by combining the cryptographic primitives physical layer attributes are developed. The security of our method is analyzed and evaluated its computational overhead and communication.

Index Terms: Selective Jamming, Denial-of-Service, Wireless Networks, Packet Classification.

1. INTRODUCTION

Wireless networks are based on the continued availability of the wireless medium to be linked with participating nodes. However, the open nature of this medium makes it vulnerable to multiple security threats. Anyone with a transceiver can spy wireless transmissions, inject spurious messages or clog legitimate. While listening and post-injection can be prevented using cryptographic methods, jamming attacks are much more difficult to counter. It has been shown to upgrade severe denial of service (DoS) attacks against wireless networks [12], [17], [36], [37]. In the simplest form of jam, the antagonist interferes with the reception of messages by transmitting a continuous signal [25] interference, or several short bursts of interference [17].

Typically, attacks interference have been considered under external threat model, in which the block is not part of the network. Under this model, interference strategies include continuous or random transmission of interfering signals high power [25], [36]. However, the adoption of a strategy of "always-on" has several disadvantages. First, the opponent has to spend a significant amount of energy to jam frequency bands of interest. Second, the continued presence of unusually high levels of interference makes this type of easy detect attacks [17], [36], [37].

Conventional anti-jamming techniques rely heavily on spread spectrum (SS) communications [25], or some form of interference avoidance (eg, frequency or spatial retreats slow hop [37]). SS techniques provide bit-level protection by spreading bits according to a secret code pseudo-noise (PN) known only to the communicating parties. These methods can only protect wireless transmissions under the model of external threat. Potential for revealing secrets of compromised node, neutralizes the benefits of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended recipients should be aware of the secrets that are used to protect transmissions. Therefore, the commitment to a single receiver is sufficient to reveal corresponding hash.

In this paper the problem of interference is discussed under an internal threat model. A sophisticated adversary who is aware of the secrets of the network and the implementation details of network protocols at any layer of the network stack is considered. The adversary his inside knowledge to launch targeted attacks interference in which specific messages "great importance" target exploits. For example, a clamp can send messages route-request/route-reply the routing layer to put off route discovery or target TCP acknowledgments in a TCP session to seriously degrade the performance of a flow from end to end.

To launch targeted attacks interference, the opponent must be able to implement a strategy of "sort-then-jam" before the end of a wireless transmission. Such strategy can be updated either by classifying packets transmitted using the protocol semantics [1], [33], or by decoding the packets on the fly [34]. In the latter method, the blocker can decode the first few bits of a packet identifier for the recovery of useful, such as packet type, source address and destination packages. After sorting, the adversary should induce a sufficient number of bit errors so that the packet cannot be recovered at the receiver [34]. Selective jamming requires intimate knowledge of the physical layer (PHY) and the specific characteristics of the upper layers.

DOI 10.17148/IJARCCE.2017.6145

Our Contributions: We investigate the possibility of packet classification in real time to launch targeted attacks interference, under a model of internal threat. We show that such attacks are relatively easy to make by exploiting the knowledge of network protocols and cryptographic primitives extracted from compromised nodes. We investigated the impact of selective blockade of critical network functions. Our findings indicate that selective jamming attacks lead to a denial of service, with very little effort on behalf of the jaw. To mitigate such attacks, two schemes that prevent the classification of packets transmitted in real time are developed. Our schemes are based on the joint consideration of cryptographic mechanisms with PHY-layer attributes. The security of our schemes is analyzed and shown to achieve strong security properties, with minimal impact on network performance.

The remainder of the paper is organized as follows. In section 2, we describe the related works. In section 3 describe the problem addressed, and state the system and adversarial model. In section 4, describe the feasibility of selective jamming attacks. In section 5, the impact of selective jamming. In section 6 and 7, develop methods for preventing selective jamming. In section 8, implementation methodology. Finally in section 9 concluded the paper.

2. RELATED WORKS

Jamming Attacks in voice communications have been launched since the 1940s [25]. In the context of digital communications, the interference problem has been addressed in several threat models. Classification based on the selective nature of the adversary is presented.

2.1 Prior work on Selective Jamming

In [33], Thuente studied the impact of an external selective jammer that targets several control packets at the MAC layer. To perform packet classification, the adversary exploits inter-packet timing information to infer packet transmissions prestige. In [11], Law et al. proposed estimating the probability distribution of transmission times between packets of different types based on analysis of network traffic packets. Future broadcasts in several layers predicted from estimated timing information. Using their model, the authors proposed strategies for selective interference networks MAC protocols well known sensors.In [1], Brown et al. the feasibility of selective interference based on the semantics of protocol is illustrated. They considered several encrypted packet identifiers as the packet size of packets, the information on the exact timing of the various protocols, and the detection of the physical signal. To avoid selectivity, the unification of packet characteristics, such as minimum length and time between packets is proposed. Classification techniques similar packages were investigated in [4].

Liu et al. considered a clever gag that takes into account specific details of protocol to optimize its blocking strategy [14]. The adversary is assumed to direct control messages at different layers of the network stack. To mitigate interference intelligently, the authors proposed the SPREAD system, which is based on the idea of stochastic selection from a collection of parallel protocols at each layer. The uncertainty introduced by this stochastic selection mitigates the selective ability of the clamp. Greenstein et al. presented a 802.11-like wireless protocol called Slyfi preventing packet classification by external observers. This protocol all explicit identifiers of packets transmitted (e.g., MAC layer header and payload) by the encryption key is known only hides that provided [8] receptors.

Interference targeted attacks have been applied experimentally engines use software-defined radio [32], [34]. Wilhelm et al. implemented a platform called RFReact USRP2 based interference that allows selective blocking and reactive [34]. RFReact proved to be agnostic to technology standards and easily adaptable to any desired locking strategy. The success rate of an attack against a selective blockade 802.15.4 network was measured to be 99.96%. Blapa et al. targeted attacks against interference studied adaptive rate mechanism of 802.11 [32]. They showed that selective targeting one specific packages jammer in 802.11 talk around was able to reduce the communication speed to the minimum value of 1 Mbps, with relatively little effort (5-8 jam packets per second). The results were verified experimentally using USRP2/GNU platform radio.

Several researchers have suggested attacks selective channel interference, in which the blocker the broadcast control channel is addressed. It has been shown that such attacks reduce the power required to perform a DoS attack by several orders of magnitude [3]. To protect traffic control channels, replication control transmission of multiple channels was proposed in [3], [30], [31]. The "locations" of the control channels, where cryptographically protected. In [12], Lazos et al. proposed a random frequency hopping algorithm for protecting the control channel jammers inside. Strasser et al. proposed a technique of frequency hopping anti-jamming that does not require the existence of a sequence of secret shared hop communication between the parties [28].

2.2 Non-Selective Jamming Attacks

Conventional methods for interference mitigation employ some form of communication of the SS [5], [25]. The transmitted signal is transmitted to a larger band width after a PN sequence. Without knowledge of this sequence, a large amount of energy (typically 20 to 30 dB gain) is required to interfere with an ongoing transmission. However, in the case of broadcast communication, compromise commonly shared PN code offsets the advantages of SS.

Popper et al. proposes a model of communication interference-resistant communications for couples who do not rely on shared secrets. Communication nodes use a modulation method uncoordinated physical layer called Direct Sequence Spread-Spectrum (UDSSS) [20]. They also proposed a method of diffusion-resistant interference

DOI 10.17148/IJARCCE.2017.6145

that transmissions according to extend the PN code of a randomly selected book public codes [20]. Several other schemes generally eliminate the need for PN secret codes [15], [29].Lin et al. showed that 13% interference of a packet is sufficient to overcome the ECC capabilities of the receiver [13]. Xu et al. jammers categorized into four types: (a) a constant gag, (b) a misleading gag transmitting messages made, (c) a random issue, and (d) reactive gag jams only if activity is detected [37] .Further studied the problem of detecting the presence of jammers by measuring performance parameters such as the ratio of the delivery of packages [35] - [37]. Cagalj et al. anti-jamming techniques based on wormholes proposed for wireless sensor networks (WSN) [2]. Using a wormhole link, sensors within the region jammed communications with external nodes and report on the ongoing attacks interference.

3. PROBLEM STATEMENT AND ASSUMPTIONS

3.1 Problem Statement

Consider the scenario shown in Fig. 1. Nodes A and B communicate via a wireless link. Within the communication range of A and B there is a jamming node J. When A transmits a packet to B m, m classifies the node J receiving only the first bytes of m. J m then corrupted beyond recovery by interfering with their reception at B. We address the problem of preventing the interference node ranking m in real time, thus mitigating the ability of J to selective blockade. Our goal is to transform a selective one random jammer. Note that in the present work, we do not address the classification methods based on the semantics of the protocol packets, as described in [1], [4], [11], [33].

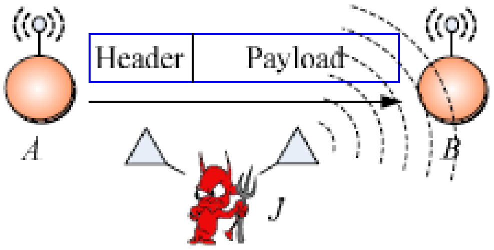


Fig. 1. Realization of a selective jamming attack

3.2 System and Adversary Model

Network model: The network consists of a collection of nodes connected by wireless links. The nodes can communicate directly if they are within communication range, or indirectly through multiple hops. The nodes communicate both unicast mode and broadcast mode. Communications can be encrypted or not. For communications encrypted broadcast, symmetric keys are shared between all of the intended recipients. These keys are established using pairwise pre-shared key or asymmetric cryptography.

Communication Model: The packets are transmitted at a baud rate R. Each symbol PHY-layer corresponds to q bits, in which the Q value is defined by the underlying digital modulation scheme. Each symbol carries α / β data bits, where α / β is the rate PHY-layer encoder. Here the transmission bit rate is equal to and QR bps bit rate information is α/βqR. Techniques such as spread spectrum frequency hopping wide (FHSS) or direct spread spectrum sequence (DSSS) can be used in the PHY layer, to protect wireless spectrum jamming transmissions. SS provides immunity to interference, to some extent (typically 20 to 30 dB gain), a potent blocker but is still capable of interference data packets of your choice.

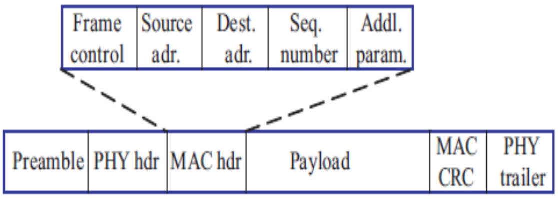


Fig. 2. A generic frame format for a wireless network

The transmitted packet is the basic format shown in FIG. 2. Preamble is used to synchronize the sampling process in the receiver. The PHY header contains information about the length of the frame, and the transmission speed. The MAC header determines the MAC version of the protocol, source address and destination sequence numbers plus some additional fields. MAC header is followed by the frame body typically contains an ARP packet or an IP datagram. Finally, the MAC frame is protected by a code of cyclic redundancy check (CRC). In the PHY layer, a trailer may be added to synchronize the transmitter and receiver.

Adversary Model: We assume that the adversary is in control of the media and messages may be stuck in any part of the network of your choice (similar to the Dolev-Yao model). The adversary can operate in full duplex mode, and being able to receive and transmit simultaneously. This can be accomplished, for example, with the use of multiple radio transceivers. In addition, the adversary is equipped with directional antennas for reception of a signal from a node and the jam of the same signal in another. For analysis purposes, assume that the adversary a number of bits just below ECC capability early in the transmission may jam proactive. He can then decide irredeemably corrupt a packet transmitted by the interference of the last symbol. Actually, it has been demonstrated that selective interference can be achieved with much less [32], [34]. A jammer equipped with one half-duplex transceiver is sufficient to classify packets transmitted and jam. However, our model captures a more powerful adversary that can be effective even at high transmission speeds. The adversary is assumed to be computationally limited storage and, although it can be much higher than normal nodes. In particular, it can be equipped with special purpose hardware to perform cryptanalysis or any other type of calculation required. Solve hard problems known cryptographic supposed to be long. For purposes of analysis, given a cipher text, the

DOI 10.17148/IJARCCE.2017.6145

most efficient way to derive the corresponding plaintext method is supposed to be an exhaustive search on the key space. The implementation details of each layer of the network stack are supposed to be public.
Moreover, the adversary is capable of instruments of compromising network and retrieval of stored information including cryptographic keys, PN codes, etc. This internal adversary model is realistic network architectures, such as mobile ad-hoc, mesh, cognitive radio and wireless sensor networks where network devices can run unattended, thus being capable of physical commitment.

4. REAL TIME PACKET CLASSIFICATION

At the physical layer, a packet m is coded, interleaved and modulated before transmission via the wireless channel. At the receiver, the signal is demodulated, de-interlacing and decryption to recover the original packet m. The nodes A and B communicate via a wireless link. Within the communication range of A and B there is a jamming node J. When A transmits a packet to B m, m classifies the node J receiving only the first bytes of m. J m then corrupted beyond recovery by interfering with their reception at B. Consider the generic communication system shown in FIG. In the PHY layer, a packet m is coded, interleaved and modulated before transmission via the wireless channel. At the receiver, the signal is demodulated, de-interleaved and decoded to recover the original packet m.

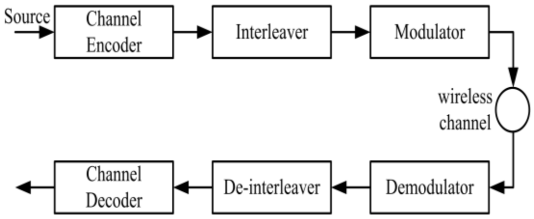


Fig. 3. A generic communication system diagram

Moreover, even if the encryption key concealment scheme be kept secret, the static parts of a packet transmitted could potentially lead to packet classification. This is because for computationally efficient methods such as block cipher encryption, the encryption of a plaintext with the same key code you get a text prefix static encryption. Thus, an adversary who is aware of the details of the underlying protocols (frame structure) can use the static text portions of a packet transmitted to classify encryption.

5. IMPACT OF SELECTIVE JAMMING

The impact of selective interference attacks network performance is illustrated in this section. We use OPNETTM Modeler 14.5 [18] to implement selective interference attacks on two stages of multi-hop wireless networks. In the first scenario, the attacker runs a route established over a wireless multi-hop TCP connection. In the second scenario, the jammer control messages directed layer transmission network during the process of establishing.

Selective jamming at the Transport Layer: In the first series of experiments, we set up a file transfer a 3 MB file between two users A and B connected via a multi-hop route. The TCP protocol is used to reliably transport the requested archive. In the MAC layer, the RTS / CTS mechanism is enabled. The transmission speed is set to 11 Mbps in each link. The clamp is placed in the proximity of one of the intermediate jumps of the TCP connection. Four interference strategies are considered: (a) interference of cumulative selective TCP-ACK, (b) selective interference RTS / CTS, (c) selective interference messages of data packets, and (d) random interference any package. In each of the strategies, a fraction p of packets addressed stuck.

Selective jamming at the Network Layer: In this scenario, we simulated a multi-hop wireless network of 35 nodes randomly placed in a square area. The AODV routing protocol is used to discover and establish routing paths [19]. Connection requests were initiated between pairs of source / destination randomly. Three jammers were strategically placed to selectively jam the network areas do not overlap. Three types of interference strategies were used: (a) a continuous gag, (b) random blocker blocking only a fraction p of the transmitted packets, and (c) a selective blocker guidance route request (RREQ) packets.

6. STRONG HIDING COMMITMENT SCHEME (SHCS)

Strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. The motivation is to satisfy the strong property while hiding computation and communication overhead is kept to a minimum. The proposed SHCS requires joint consideration of the MAC and PHY layers. To reduce the overhead of SHCS, the value of commitment d (i.e., the decryption key k) is performed in the same package as the value C. committed to achieving strong hiding property, a sub layer called "concealment layer sub "is inserted between the MAC and PHY layers. This sub layer is responsible for formatting m before it is processed by the PHY layer. A Framework m delivery at the MAC layer to layer sub hideout. Frame m consists of a MAC header and the payload, followed by the trailer containing a CRC code. The computational overhead of SHCS symmetric encryption is one transmitter and one in the symmetric decryption in the receiver. Because the header information is permuted and encrypted as a trailer, all receivers in the vicinity of a sender should receive the entire packet and decrypt it before package type and destination can be determined.

7. ALL-OR-NOTHING TRANSFORMATION (AONT)

The proposed changes based on all-or-nothing, which introduces a modest communication and computation overhead solution. These changes were originally proposed by rivets to curb brute-force attacks against

DOI 10.17148/IJARCCE.2017.6145

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering

ISO 3297:2007 Certified

Vol. 6, Issue 1, January 2017

encryption algorithms block packets are decoded by an AONT before transmission, but remain unencrypted. The jammer cannot perform packet classification until they have received all the messages for the original package and pseudo inverse transformation has been applied AONT serves as a pre-processing of public knowledge and fully invertible to text clear before it becomes a common block cipher algorithm. A transformation f, mapping message m = {m1; . . .; mx} a sequence of pseudo plain text messages are pre-processed by an AONT before encoding, all ciphertext blocks must be received for any part of the plaintext. Therefore, brute force attacks are slowed by an equal number of ciphertext blocks factor, without any change in the size of the secret key.

8. IMPLEMENTATION

The runtime has a JDK software that runs on the Windows operating system. The system uses the technology as Java RMI (Remote Method Invocation). SWING Java API is used to create the user interface. The RMI technology allows nodes to communicate remotely. The simulation has three types of nodes namely centralized server, client and server. The purpose of the source is sending data to the destination. There sender will be consisting of the channel encoder, interweaver and modulator. For the simulation of communication in WSN, the node server is able to send messages to the client nodes based on the port number and communication is routed through one of the centralized servers. Here the user can select a file by clicking the Browse button. The Send button will be initiated by the user in order to send messages to customers based on port number. The message or file is divided into packets with length of 48 bytes.

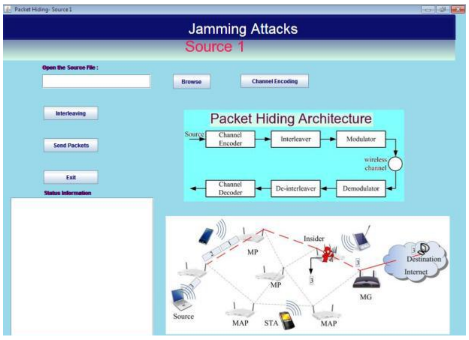
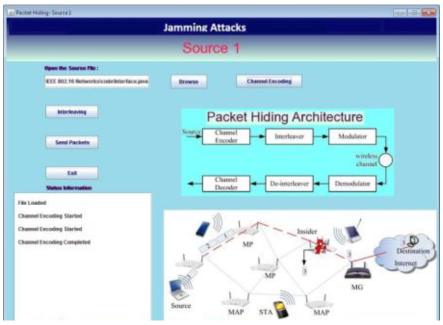


Fig.4 screen shot for source



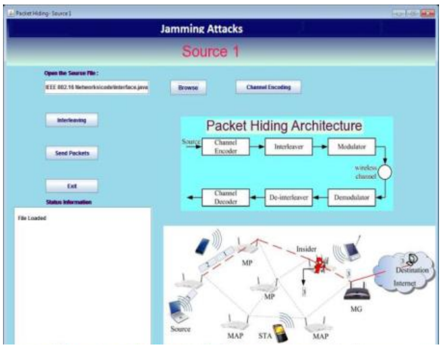
IEEE 802.16 Networks\code\Interface.java

File Loaded
Channel Encoding Started
Channel Encoding Started
Channel Encoding Completed

Fig .5 File loading

The required data is selected and sent to a particular client. Data is sent in packets with a length of 48 bytes. The server has to use the IP address and specific port number based on the centralized server through which the message is sent to the client. Select the data to be transferred by clicking the Browse button.

After selecting the file, click the channel encoder. Channel coding control handles errors during transmission through the communication channel. The information sequence to the encoded sequence is transformed. The result we get after modulation is "code word." Code word is an element of a standardized code or protocol. Each code word is assembled according to the specific rules of the code and is assigned a unique meaning. Keywords are typically used for reasons of reliability, clarity, brevity, or secrecy.

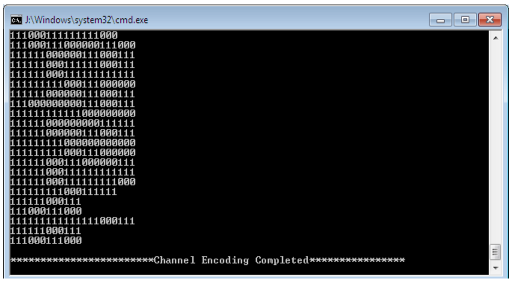


IEEE 802.16 Networks\code\Interface.java

File Loaded

Fig.6 Acknowledgment for loading File

The purpose of the coding theory is to find the channel which rapidly transmitted codes contain many valid code words and can be corrected or at least detect many errors. While not mutually exclusive, performance in these areas is a compromise. Thus, different codes are optimal for different applications. Channel coding is performed in this manner. After coding is completed a message will be displayed.



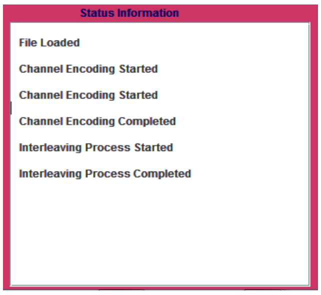
```
111000111111111000
1110001110000000111000
1111110000000111000111
1111110001111111000111
1111110001111111111111
1111111110001110000000
1111110000000111000111
1110000000000111000111
1111111111111000000000
1111110000000000111111
1111110000000111000111
1111111110000000000000
1111111110001110000000
1111110001110000000111
1111110001111111111111
1111110001111111111000
111111111000111111
111111000111
111000111000
1111111111111111000111
111111000111
111000111000

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

Fig.7 Channel encoding of the data

Collate, a technique to make error correction forward more robust to burst errors. Interleaving is a way of organizing data in a non contiguous way to increase performance. The error correction coding, particularly within data transmission, disk storage, and memory. After the interleaved data is converted into packets. Then, packets for transmission are used. Interleaving the bits of the binary representation of the coordinate values to produce a Z order (curve) through the points.

DOI 10.17148/IJARCCE.2017.6145

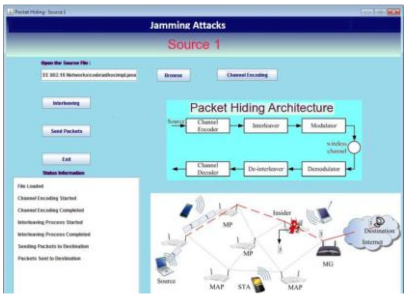


Status Information

File Loaded
Channel Encoding Started
Channel Encoding Started
Channel Encoding Completed
Interleaving Process Started
Interleaving Process Completed

Fig.8 Status Corresponding to particular action

Identify the destination and the data is converted into packets and sent to the selected destination. If the data are sent correctly, there will be a message on the "Status Information".

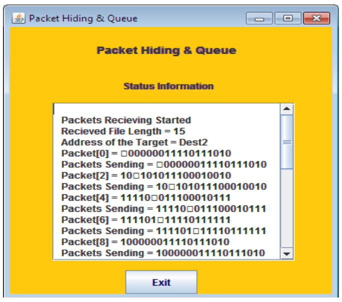


File Loaded
Channel Encoding Started
Channel Encoding Completed
Interleaving Process Started
Interleaving Process Completed
Sending Packets to Destination
Packets Sent to Destination

Fig.9 Packet Transmission to the Packet hiding queue

8.1 Packet Hiding

Package hiding Cola is responsible for sending packets in a format that is queue in order of arrival of the first arriving packets will be sent for the first time in a sequential order. Hiding packet acts as a server that is used to identify the destination. Also check the size of the data when we are transmitting. Each package the information is stored in binary format. The packet queue concealment is responsible for sending data to the destination.

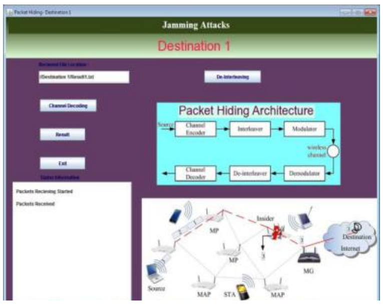


Packet Hiding & Queue

Status Information

```
Packets Recieving Started
Recieved File Length = 15
Address of the Target = Dest2
Packet[0] = □000000111101110 10
Packets Sending = □0000001111011101 0
Packet[2] = 10□101011100010010
Packets Sending = 10□101011100010010
Packet[4] = 11110□011100010111
Packets Sending = 11110□011100010111
Packet[6] = 111101□11110111111
Packets Sending = 111101□11110111111
Packet[8] = 100000011110111010
Packets Sending = 100000011110111010
```

Fig.10 Packet Hiding Queue



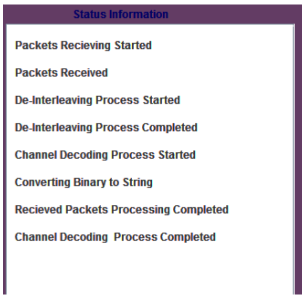
\Destination 1\Result1.txt

Packets Recieving Started
Packets Received

Fig.11 Packets Received at Destination

As the concealment queue sends data packets received from the source to the destination. The destination will be ready to take data queue hiding packet.

The target is to receive the route where you can get the queue data hiding packages. The destination will be consistent in the demodulator, De-interleaving and channel decoder. Demodulation is a process used in the receivers to recover the original signal coming from the sender end in modular fashion. At the receiving end, the interleaved data is available back to the original collation sequence. As a result of interleaving, the correlated noise introduced in the transmission channel seems to be statistically independent at the receiver and therefore allows a better correction.



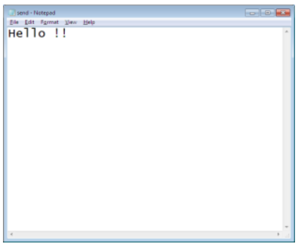
Status Information

Packets Recieving Started
Packets Received
De-Interleaving Process Started
De-Interleaving Process Completed
Channel Decoding Process Started
Converting Binary to String
Recieved Packets Processing Completed
Channel Decoding Process Completed

Fig. 12 Status After demodulation, interleaving and channel decoding

8.2 File data at the Source

Data sent from the sender is a text file that is consistent with the following information.

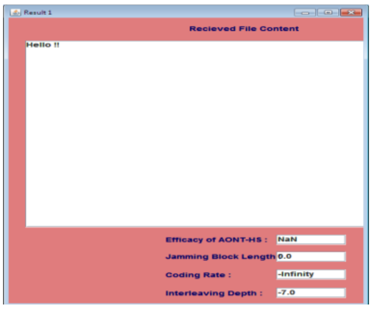


Hello !!

Fig 13 Choose file with the data at Source

8.3 Destination

The text area is state information for the submission of status messages.



Recieved File Content

Hello !!

Efficacy of AONT-HS : NaN
Jamming Block Length 0.0
Coding Rate : -Infinity
Interleaving Depth : -7.0

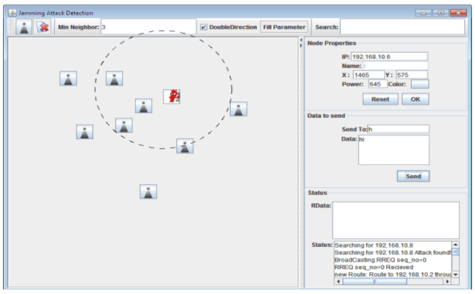
Fig.14 Received data at the destination

8.4 The Jamming Attack Analysis

Experiments were performed with two clients, two servers and a tail packet concealment. The communication flow

DOI 10.17148/IJARCCE.2017.6145

starts when the source decides to send messages to the client. Select a file and breaks it into many packages of size 48 bytes each, and sent through the centralized server randomized. The communication server monitors and detects any attack interference. Attacks interference can see "Analysis of Jamming attack" when data is sent from source to destination using stealth tail packets. It is able to analyze the attacks and also to know if the attack is made or not. Estimated packet loss. It is assumed that due to attacks by sending packets may occur and, in turn gives rise to data loss or the packet loss.



Min Neighbor: 3
☑ DoubleDirection
IP: 192.168.10.6
X: 1465 Y: 575
Power: 645 Color:
Send To: h
Data: hi
Status: Searching for 192.168.10.8
Searching for 192.168.10.8 Attack found!
BroadCasting RREQ seq_no=0
RREQ seq_no=0 Recieved
new Route: Route to 192.168.10.2 throu

Fig.15 Jamming Attack Detection

As seen in Figure 15, the interference when the attack is detected, then it will be indicated with the red symbol on the corresponding node.

9. CONCLUSION

We addressed the problem of selective interference attacks on wireless networks. We consider a model of internal adversary where the jammer is part of the network under attack, being therefore the protocol specifications and network shared secrets. We have shown that the jammer can classify packets transmitted in real time by decoding the first symbols of a transmission in progress. The impact of selective jamming attacks on network protocols such as TCP and routing was evaluated. Our results show that a selective jammer can significantly affect performance with little effort. We have developed two schemes that transform a selective blocker for random by preventing packet classification in real time. Our schemes combine cryptographic primitives such as commitment schemes and transformations of all-or-nothing (AONTs) with physical layer characteristics. We have analyzed the security of our schemes and quantify the overhead of computation and communication.

REFERENCES

1. 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.
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. 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.
5. Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.
6. K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES. Cryptographic Engineering, pages 235–294, 2009.
7. O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004.
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. IEEE. IEEE 802.11 standard. http://standards.ieee.org/getieee802/download/802.11-2007.pdf, 2007.
10. A. Juels and J. Brainard. Client puzzles: A cryptographic counter measure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.
11. 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.
12. 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.
13. G. Lin and G. Noubir. On link layer denial of service in data wireless LANs. Wireless Communications and Mobile Computing, 5(3):273–284, May 2004.
14. X. Liu, G. Noubir, and R. Sundaram. Spread: Foiling smart jammers using multi-layer agility. In Proceedings of INFOCOM, pages 2536– 2540, 2007.
15. Y. Liu, P. Ning, H. Dai, and A. Liu. Randomized differential DSSS: Jamming-resistant wireless broadcast communication. In Proceedings of INFOCOM, San Diego, 2010.
16. R. C. Merkle. Secure communications over insecure channels. Communications of the ACM, 21(4):294–299, 1978.
17. G. Noubir and G. Lin. Low-power DoS attacks in data wireless lans and countermeasures. Mobile Computing and Communications Review, 7(3):29–30, 2003.
18. OPNET. OPNETtm modeler 14.5. http://www.opnet.com/.
19. C. Perkins, E. Belding-Royer, and S. Das. RFC 3561: Ad hoc ondem and distance vector (AODV) routing. Internet RFCs, 2003.
20. C. P¨opper, M. Strasser, and S. ˇCapkun. Jamming-resistant broadcast communication without shared keys. In Proceedings of the USENIX Security Symposium, 2009.
21. R. Rivest. All-or-nothing encryption and the package transform. Lecture Notes in Computer Science, pages 210–218, 1997.
22. R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timedrelease crypto. Massachusetts Institute of Technology, 1996.
23. B. Schneier. Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, 2007.
24. SciEngines. Break DES in less than a single day. http://www.sciengines.com, 2010.
25. M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.
26. D. Stinson. Something about all or nothing (transforms). Designs, Codes and Cryptography, 22(2):133–138, 2001.
27. D. Stinson. Cryptography: theory and practice. CRC press, 2006.
28. M. Strasser, C. P¨opper, and S. ˇCapkun. Efficient uncoordinated fhss anti-jamming communication. In Proceedings of MobiHoc, pages 207–218, 2009.
29. M. Strasser, C. P¨opper, S. ˇCapkun, and M. Cagalj. Jamming-resistant key establishment using uncoordinated frequency hopping. In Proceedings of IEEE Symposium on Security and Privacy, 2008.
30. P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of control channel jamming via random key distribution. In Proceedings of PIMRC, 2007.
31. 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.
32. 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.
33. D. Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.

DOI 10.17148/IJARCCE.2017.6145