IJRRECS/March 2015/Volume-3/Issue-3/3801-3805 **ISSN 2321-5461**

INTERNATIONAL JOURNAL OF REVIEWS ON RECENT ELECTRONICS AND COMPUTER SCIENCE

SECURITY MEASURES AGAINST UNCERTAIN WIRELESS CHANNELS

K.RAVIKUMAR[1], N.KRISHNAIAH[2]

[1]M.Tech Student, Dept of CSE, BVCEC, Odalarevu, A.P, India

[2]Associate Professor, Dept of CSE, BVCEC, Odalarevu, A.P, India

ABSTRACT:

Jamming attacks might be sighted as an extraordinary case of Denial of service attacks. In recent times, quite a lot of alternative jamming schemes were demonstrated. Jamming attacks in general were measured under representation of external threat, in which they transmits constant or random high power interference signals; however these types of strategies contain quite a lot of disadvantages. In our work we consider jamming attacks under a representation of internal threat. Selective jamming attacks are comparatively simple to actualize by using knowledge of network protocols as well as cryptographic primitives that are extracted from compromised nodes. To commence selective jamming attacks, adversary should be able to implement a classify-then-jam scheme earlier than completion of wireless transmission. To alleviate such attacks, we build up three schemes that put off classification concerning transmitted packets in real time. These schemes depend on joint consideration of cryptographic mechanisms by PHY-layer attributes and they attain tough security properties, with negligible impact on the network performance.

Keywords: Jamming attacks, Denial of service attacks, Selective jamming, Wireless transmission, Cryptography, Packets.

1. INTRODUCTION:

Wireless networks functions as transport means among devices and because of this these are prone to numerous security threats due to the open nature. One of the most important severe security threats is jamming of wireless communications and degrading

network performance [1]. Jamming occurs as noise or else interference at the receiver side and can disturb wireless transmission. Attacker interferes in simple jamming with set of frequency bands used for communication by conveying a constant jamming signal. Jamming attacks in general were measured under representation of external threat, in which they transmits constant or random high power interference signals; however these types of strategies contain quite a lot of disadvantages. First, attacker needs to use vast amount of energy to jam convinced frequency bands; secondly, because of constant presence of high interference levels, these attacks are simple to detect. In our work we consider jamming attacks under a representation of internal threat. Selective jamming attacks directs to a DoS with extremely low effort in support of jammer. To alleviate such attacks, we build up three schemes that put off classification concerning transmitted packets in real time. We put forward a strong hiding commitment system that is on basis of symmetric cryptography; present a packet hiding system on basis of cryptographic puzzles and put forward a solution on basis of All-Or-Nothing Transformations that set up a modest communication as well as computation transparency [2]. We consider a complicated adversary who is conscious of network secrets and performance details of network protocols at any layer within network stack. He exploits internal knowledge for initiation of selective jamming attacks in which particular messages of more significance are targeted.

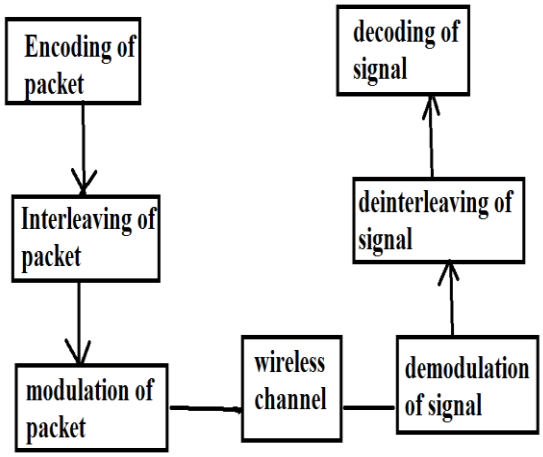

Fig1: Generic communication structure

2. METHODOLOGY:

Jamming attacks might be sighted as an extraordinary case of Denial of service attacks. Continuous jamming was used as a denial-of-service attack against voice communication. In recent times, quite a lot of alternative jamming schemes were demonstrated. Existing anti-jamming techniques depend broadly on spread-spectrum communications which offer bit-level security by spreading bits in proportion to a secret pseudo-noise (PN) code, well-

known only to communicating parties. These methods can defend wireless transmissions under external threat representation. Broadcast communications are mainly susceptible under an internal threat representation since all intended receivers must be conscious of secrets used to defend transmissions. To commence selective jamming attacks, adversary should be able to implement a classify-then-jam scheme earlier than completion of wireless transmission. Such schemes can be actualized moreover by classifying transmitted packets by means of protocol semantics or by means of decoding packets on the fly. Selective jamming necessitates intimate information of physical (PHY) layer, and specifics of upper layers [3]. We assume adversary is in control of communication medium and jams messages at any part of network of his model. The adversary functions in full-duplex mode consequently accept and conveys at the same time. Internal adversary representation is practical for network architectures where network devices might function unattended, consequently being vulnerable to physical compromise. Consider the generic communication structure as shown in fig1. At PHY layer, encoding, interleaving, and modulation of packet was done prior to it is transmitted above the wireless channel. At receiver side, demodulation of signal and DE interleaving takes place, and finally decoded, to improve original packet. Selective jamming attacks are comparatively simple to actualize by using knowledge of network protocols as well as cryptographic primitives that are extracted from compromised nodes [4]. Selective jamming attacks directs to a DoS with extremely low effort in support of jammer. To alleviate such attacks, we build up three schemes that put off classification concerning transmitted packets in real time. These schemes depend on joint consideration of cryptographic mechanisms by PHY-layer attributes and they attain tough security properties, with negligible impact on the network performance.

3. SCHEMES FOR PREVENTION OF SELECTIVE JAMMING:

The difficulty of real-time packet classification is mapped towards hiding property of commitment methods, and put forward a packet-hiding scheme on basis of commitments. We put forward a strong hiding commitment system (SHCS) that is on basis of symmetric cryptography. Our

main motivation is to convince tough hiding property while maintenance of computation as well as communication transparency to a least amount. The projected SHCS necessitates consideration of MAC as well as PHY layers. To attain the well-built hiding property, a sublayer named as hiding sublayer is introduced among MAC as well as PHY layer. We present a packet hiding system on basis of cryptographic puzzles. The most important idea behind such puzzles is to compel the recipient of a puzzle to implement a pre-defined set of computations prior to extraction of a secret of interest. The time necessary for obtaining explanation of a puzzle depends on its inflexibility as well as computational capability of solver. The benefit of puzzle based system is that its protection does not depend on parameters of PHY layer. On the other hand it has superior computation as well as communication overhead. We employ cryptographic puzzles to temporary conceal transmitted packets. Additionally, the puzzle generation necessitate considerably less computation when compared to puzzle solving. We put forward a solution on basis of All-Or-Nothing Transformations (AONT) that set up a modest communication as well as computation transparency [5]. Such transformations were originally projected to decelerate brute force attacks in opposition to obstruct encryption algorithms. An AONT scheme functions as a publicly identified and totally invertible pre-processing step to a plaintext prior to passing towards an ordinary block encryption algorithm. When a plaintext is pre-processed by means of AONT before encryption, the entire cipher text blocks should be received to get hold of any part of plaintext consequently, brute force attacks are decelerated by means of a factor equivalent to number of ciphertext blocks, devoid of any change on size of secret key [6].

4. CONCLUSION:

In wireless networks, one of the most important severe security threats is jamming of wireless communications and degrading network performance. Existing anti-jamming techniques depend broadly on spread-spectrum communications whihc can defend wireless transmissions under external threat representation. Broadcast communications are mainly susceptible under an internal threat representation since all intended receivers must be conscious of

secrets used to defend transmissions. In our work we consider jamming attacks under a representation of internal threat. We consider a complicated adversary who is conscious of network secrets and performance details of network protocols at any layer within network stack. Selective jamming necessitates intimate information of physical (PHY) layer, and specifics of upper layers. Selective jamming attacks directs to a DoS with extremely low effort in support of jammer. To alleviate such attacks, we build up three schemes that put off classification concerning transmitted packets in real time. We put forward a strong hiding commitment system (SHCS) that is on basis of symmetric cryptography. We present a packet hiding system on basis of cryptographic puzzles. We put forward a solution on basis of All-Or-Nothing Transformations (AONT) that set up a modest communication as well as computation transparency. These schemes depend on joint consideration of cryptographic mechanisms by PHY-layer attributes and they attain tough security properties, with negligible impact on the network performance.

REFERENCES

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

[2] R. Rivest, A. Shamir, and D. Wagner. Time-lock puzzles and timedrelease crypto. Massachusetts Institute of Technology, 1996.

[3] B. Schneier. Applied cryptography: protocols, algorithms, and source code in C. John Wiley & Sons, 2007.

[4] SciEngines. Break DES in less than a single day. http://www.sciengines.com, 2010.

[5] M. K. Simon, J. K. Omura, R. A. Scholtz, and B. K. Levitt. Spread Spectrum Communications Handbook. McGraw-Hill, 2001.

[6] D. Stinson. Something about all or nothing (transforms). Designs, Codes and Cryptography, 22(2):133–138, 2001.