International Journal of Advanced Computer Research (ISSN (print): 2249-7277 ISSN (online): 2277-7970)
Volume-3 Number-4 Issue-13 December-2013

A new Approach for Averting Jamming Invasion with Packet Hiding Methods

M.Ramabai[1], E.Komalavalli[2]

Abstract

Wireless networks dependent on the active nodes which are reciprocally connected to uninterrupted availability of the wireless environment. Any person with a device which transmits and receives radio signals can secretly read those transmitted lines on wireless transmissions and put some bogus information, or stop legitimate ones. The surroundings of wireless medium is exposed to predictable interruption attacks which are referred as jamming. With wireless transmissions this predictable interruption can be used as launch pad for increasing Denial of Service attacks on wireless network. The internal information of procedure specifications and network secrets with challengers can launch low-effort jamming attacks which are difficult to distinguish and oppose. A condition of particular jamming attacks in wireless networks is shown in this paper. At the physical layer by performing real time packet classification the selective jamming attacks can be launched are demonstrated. By combining cryptographic primitives with physical-layer attributes we expand three schemes that prevent real time packet classification in order to moderate these attacks.

Keywords

Jamming Attacks, Denial of Service, Wireless Sensor Networks, Physical Layer, Selective Attack, Packet Hiding Methods, Routing.

1. Introduction

In general, jamming invasions have been considered under an outside hazard model, in which the jammer is not part of the network. Jamming approaches include the constant or indiscriminate transmission of high power interference signals under this model [4]. The easiest way to do this is simply to download the template, and replace the content with your own.

This work was supported in part by the Department of Computer Science Engineering, MGIT, Hyderabad, India.

M.Ramabai, Professor, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, A.P, India.

E.Komalavalli, M.Tech Student, Dept of CSE, Mahatma Gandhi Institute of Technology, Hyderabad, A.P, India.

However, adopting an "always-on" strategy has a number of drawbacks. First, in order to jam frequency bands of interest the adversary has to use a considerable amount of energy. Secondary, the unchanging mode of unusual high intervention levels makes this type of attacks easy to identify. The spread-spectrum (SS) transmissions or jamming fudging rely on anti-jamming methods. By stretching bits appropriate to a secret pseudo-noise (PN) code the SS methods afford bit-level protection, known only to the communicating nodes [1] [8]. Beneath the external attack model these techniques can only guard wireless transmissions. The difficulty of jamming beneath an internal attack model is illustrated in this paper. A complex attacker who is aware of network secrets and the execution details of network standards are measured at any layer in the network stack [11].

The opponent takes advantage of his inner data for presenting selective jamming attacks in which particular jamming attacks in which specific messages of "high importance" are targeted [17].

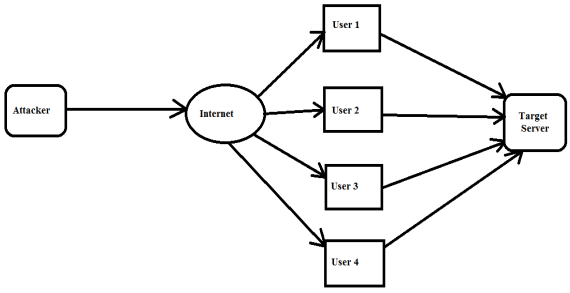

Fig 1: Denial of Service Attacks

The adversary must be capable of implementing a "classify-then-jam" strategy before the completion of a wireless transmission by launching selective jamming attacks [3]. For introducing the selective jamming attacks beneath an internal attack model the capability of real time packet classification are examined. By understanding specific information of network procedures and cryptographic basics obtain from weaken nodes are comparatively easy to describe, such attacks are projected here [9] [14]. The effect of selective jamming is examined on decisive network functions. With very low effort on behalf of

the jammer the selective jamming attacks has lead to a denial of service is shown in Fig 1 is indicated by our findings [7]. We propose three techniques that impede process of transmitted packets in real time to reduce such attacks. The mutual analysis of cryptographic techniques with PHY-layer elements is dependent on our schemes.

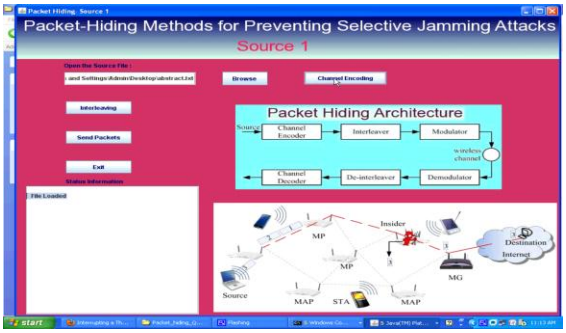

Fig 2: Select the file for channel encoder process

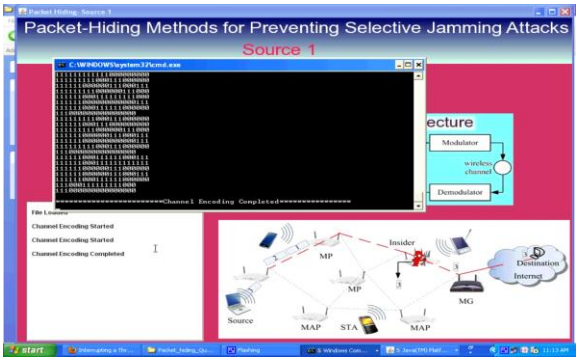

Fig 3: interleaving and Modulator process

2. Description of System and Adversary Models

Terminals may engage in conversation directly if they are within broadcasting range or accidentally by using several hops [19]. Influence can be either in plain text or cipher text. Nodes can converse in both uncast mode and transmit mode. For cipher text transfer influences, symmetric keys are split among all expected receivers. These keys are identified using pre shared pair wise keys or irregular cryptography [2] [15]. We accept the opponent is in limit of the communication medium and can crush messages at any part of the network. By using wireless sensor networks with multi-task communication, the inference of jamming at the physical layer rebound into the upper layer protocols. Opponents that are deliberate of higher-layer functionality can modify any entered information to cause the impact or reduce the resource threat for attack success. The adversary can operate in full-duplex mode which is in control of the communication medium and can jam the messages at any part of the network, thus being able to receive and transmit simultaneously [12]. We expect that the opponent can act in advance to jam a number of bits. However, a more effective adversary that can be efficient even at high transmission speeds is captured by our model. A single half-duplex transmitter is needed to arrange and stop transmitted packets with a jammer. Regardless of the fact that he can be far immune to normal nodes as the opponent is pretended to be computationally and storage bounded. Special purpose hardware is used to carry cryptography or any other required computation and they are pretended to be time ardent [5] [16].

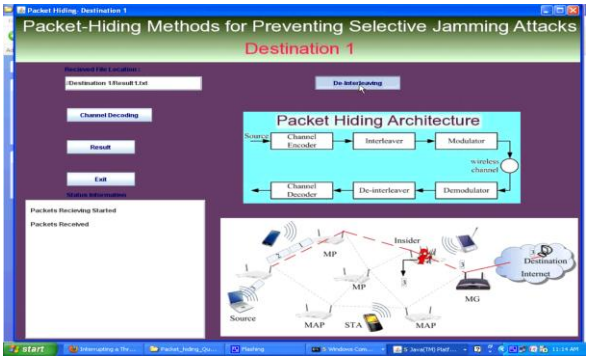

Fig 4: receiving the file at destination node

The most effective method for obtaining the associating plaintext is pretended to be a thorough search on the key space by examining the given cipher text. The flexible network devices and improving stored information including cryptographic keys, PN codes are refined by the opponent.

3. An overview of selective and non-selective jamming attacks

Selective Jamming Attacks

The effect of an exterior selective jammer who attacks several authoritative packets at media access control layer is studied. The adversary exploits inter-packet timing information to infer eminent packet transmissions to perform packet classification. For different packet types based on network traffic

analysis the estimation of the probability distribution ofinter-packettransmission times is carried out [10]. Using evaluated timing information future transmissions at several layers were stated. The unification of packet characteristics such as the smallest length and inter-packet timing was examined to prevent selectivity [6] [13]. Related packet arranging methods were examined. At different layers of the network stack the adversary was assumed to target control messages. The SPREAD system was implemented to mitigate smart jamming, which is based on the idea of stochastic selection between collections of parallel protocols at each layer.

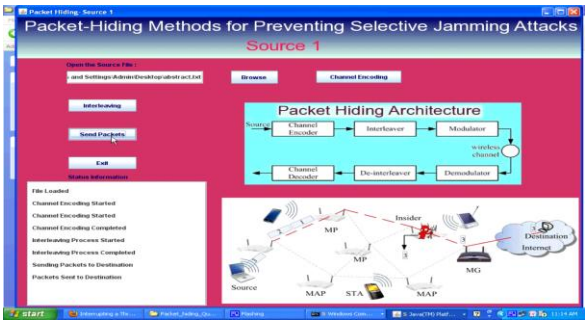

Fig 5: Sending the packets to Demodulation phase Non-Selective Jamming Attacks

Some form of SS communications can be employed by mitigating jamming with conventional methods [18]. A large amount of energy is required to interfere with an ongoing transmission as the signal which is sent is distributed to a greater data transmission rate along with PN continuous series without the knowledge of this sequence. However, with the compromise of commonly shared PN codes neutralizes the advantages of SS in the case of broadcast communications.

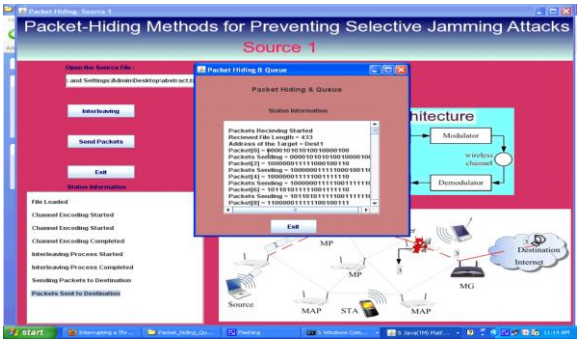

Fig 6: Packet hiding and Queue process

Corresponding nodes use a physical layer modulation method called Uncoordinated Direct- Sequence Spread Spectrum (UDSSS). A jamming-resistant broadcast method is also implemented in which transmissions are spread according to PN code randomly selected from a public codebook. Various other strategies remove mostly the need for secret PN codes. Sensors within the jammed region establish communications with outside nodes using a wormhole link and notify those regarding ongoing jamming attacks.

4. Results

The impact of attacks of selective jamming on the network performance was examined. An OPNETTM Modeller 14.5 was used to execute the attacks of selective jamming. In the Selective Jamming atthe Network Layer a multi-hop wireless network of 35 nodes were simulated which are randomly placed within a square area. The routing protocol of AODV was used to notice routing paths. Three jammers were intentionally placed to selectively jam non-overlapping areas of the network. Three types of jamming strategies were considered such as: a continuous jammer, a random jammer, blocking only a fraction of the transmitted packets, and a selective jammer targeting route request (RREQ) packets. In the given Fig[7] the number of connections established were shown, which are normalized over the number of connections in the absence of the jammers. A selective jamming attack as opposed to RREQ messages is tranquil to a persistent jamming attack.

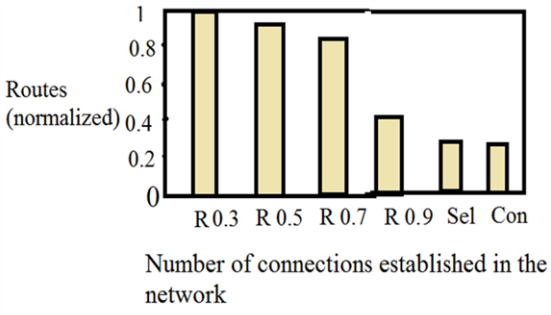

Fig 7: Connections in the network

5. Conclusion

For the increasing the Denial of Service attacks on wireless network the anticipated interruption with wireless transmissions can be used as launch pad is shown in this paper. A related opponent model in

which the attacker is part of the network beneath the attack is considered. By deciphering the first few symbols of an on-going transmission of the transmitted packets in real time are arranged by the jammer are shown here. The difficulty of selective jamming attacks in wireless networks is characterized in this paper. The three schemes that alter a selective jammer to a random one by preceding real-time packet classification are enlarged. The security and determined process of computing and transmission originating of our schemes are examined.

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 anti-jamming 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 countermeasure 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. ACMTransactions 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. Com- munications 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 ondemand distance vector (AODV) routing. Internet RFCs, 2003.

Dr. M. Rama Bai received, her B.E degree from Bharathiar University, Coimbatore(T.N) and her M.Tech (CSE) from College of Engineering, Osmania University, Hyderabad. She received her Ph.D. degree in Computer Science from Jawaharlal Nehru Technological University, Kakinada (JNTUK) in 2012. She joined as Assistant Professor in the Dept of Computer Science & Engineering, Mahatma Gandhi Institute of Technology (MGIT) in 1999. At present she is working as Professor in Dept of CSE, MGIT, Hyderabad, AP. Her research interests includes Image Processing, Pattern Recognition, Digital Water Marking and Image Retrieval Systems. She has published 20 research publications in various National, International conferences, proceedings and Journals. She has a total teaching experience of 18 years. She is a life member of ISTE.

E.KomalValli is pursuing her M.Tech (CN&IS) from Mahatma Gandhi College of Engineering, Hyderabad. Her research interest includes Computer Networks, Information security, Image Processing and Pattern Recognition.