ISSN (Online) 2394-2320

International Journal of Engineering Research in Computer Science and Engineering (IJERCSE)
Vol 5, Issue 3, March 2018

Preventing Selective Jamming Attacks by Packet-Hiding Method Using Ns-2

[1] Ganesh R.Patil, [2] Rajesh B. Khotre, [3] Gitanjali S. Korgaonkar
[1][2][3] Assistant Professor,Department of Electronics &Telecommunication Engg, PVPPCOE,Sion,Mumbai (India)

Abstract: **- The wireless networks are more sensitive to the Denial-of-Service (DoS) attacks. The existing system is based on Spread Spectrum (SS). This technique mainly focuses on an external threat model. In wireless network the communications between nodes take place through broadcast communication. That is why, if an attacker present within the network can easily eavesdrop the message sent by any node. The performance of the proposed scheme is to be evaluated through a series of simulations with the ns-2 network simulator.**

Keywords:- **Jammer,Nodes.**

I. INTRODUCTION

The network consists of a collection of nodes connected via wireless links.Nodes may communicate directly if they are within communication range,or indirectly multiple hopes.Nodes communicate both in unicast mode and broadcast mode.Communication can be either unencrypted or encrypted.For encrypted broadcast communications,sysmetric krys are shred among all intended receivers.These keys are established using preshared pairwise keys or asysmetric cryptography.Conventional anti-jamming techniques rely extensively on spread-spectrum (SS) communications or some form of jamming evasion (e.g., slow frequency hopping, or spatial retreats). SS techniques provide bit-level protection by spreading bits according to a secret pseudo-noise (PN) code, known only to the communicating parties. These methods can only protect wireless transmissions under the external threat model.We illustrate the impact of selective jamming attacks on the network performance. We used OPNET Modeler 14.5 to implement selective jamming attacks in two multihop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multihop wireless route. In the second scenario, the jammer targeted network-layer control messages trans- mitted during the route establishment process.The performance of the proposed scheme is to be evaluated through a series of simulations with the ns-2 network simulator.

II. EXİSTİNG SYSTEM

Jamming attacks are much harder to counter and more security problems. They have been shown to actualize severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the adversary interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses jamming attacks have been considered under an external threat model, in which the jammer is not part of the network. Under this model, jamming strategies include the continuous or random transmission of high power interference signals.

III.PRAPOSED SYSTEM

In this research paper, we address the problem of jamming under an internal threat model. We consider a sophisticated adversary who is aware of network secrets and the implementation details of network protocols at any layer in the network stack. The adversary exploits his internal knowledge for launching selective jamming attacks in which specific messages of “high importance” are targeted. For example, a jammer can target router request/ route-reply messages at the routing layer to prevent route discovery, or target TCP acknowledgments in a TCP session to severely degrade the throughput of an end-to-end flow. To launch selective 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, or by decoding packets on the fly. 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 [14]. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.

3.1 MODULES

1. NETWORK MODULES

We address the problem of preventing the jamming node from classifying m in real time, thus mitigating J's ability to perform selective jamming. The network consists of a collection of nodes connected via wireless links. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops. Nodes communicate both in Unicast mode and broadcast mode. Communications can be either unencrypted or encrypted. For encrypted broadcast communications, symmetric keys are shared among all intended receivers. These keys are established using pre shared pair wise keysor asymmetric cryptography.

2. REAL TIME PACKET CLASSIFICATION

Consider the generic communication system depicted in Figure 4. At the PHY 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.

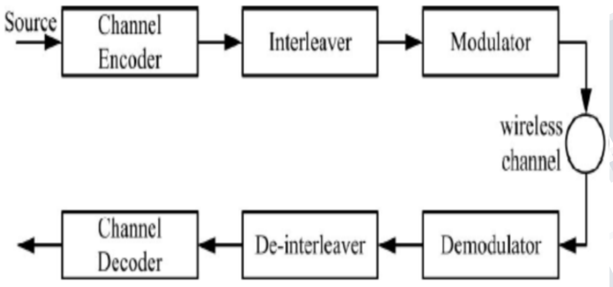

Fig 1

Moreover, even if the encryption key of a hiding scheme were to remain secret, the static portions of a transmitted packet could potentially lead to packet classification. This is because for computationally-efficient encryption methods such as block encryption, the encryption of a prefix plaintext with the same key yields a static cipher text prefix. Hence, an adversary who is aware of the underlying protocol specifics (structure of the frame) can use the static cipher text portions of a transmitted packetto classify It.

3. SELECTIVE JAMMING MODULE

We illustrate the impact of selective jamming attacks on the network performance. Implement selective jamming attacks in two multi-hop wireless network scenarios. In the first scenario, the attacker targeted a TCP connection established over a multi-hop wireless route. In the second scenario, the jammer targeted network-layer control messages transmitted during the route establishment process selective jamming would be the encryption of transmitted packets (including headers) with a static key. However, for broadcast communications, this static decryption key must be known to all intended receivers and hence, is susceptible to compromise. An adversary in possession of the decryption key can start decrypting as early as the reception of the first cipher text block.

4. STRONG HIDING COMMITMENT SCHEME (SHCS)

We propose a strong hiding commitment scheme (SHCS), which is based on symmetric cryptography. Our main motivation is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum.

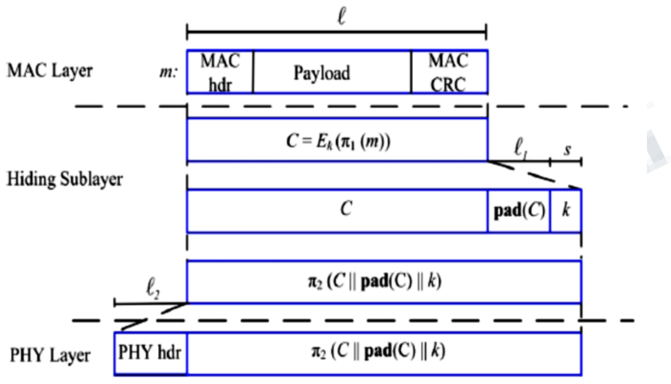

Fig 2

The computation overhead of SHCS is one symmetric encryption at the sender and one symmetric decryption at the receiver. Because the header information is permuted as a trailer and encrypted, all receivers in the vicinity of a sender must receive the entire packet and decrypt it, before the packet type and destination can be determined [17]. However, in wireless protocols such as 802.11, the complete packet is received at the MAC layer before it is decided if the packet must be discarded or be further processed. If some parts of the MAC header are deemed not to be useful information to the jammer, they can remain unencrypted in the header of the packet, thusavoiding the decryption operation at the receiver.

5. CRYPTOGRAPHIC PUZZLE HIDING SCHEME (CPHS)

We 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 PHY layer parameters. However, it has higher computation and communication overhead [4]. We consider several puzzle schemes as the basis for CPHS. For each scheme, we analyze the implementation details which impact security and performance. Cryptographic puzzles are primitives originally suggested by Merkle as a method for establishing a secret over an insecure channel. They find a wide range of applications from preventing DoS attacks to providing broadcast authentication and key escrow schemes.

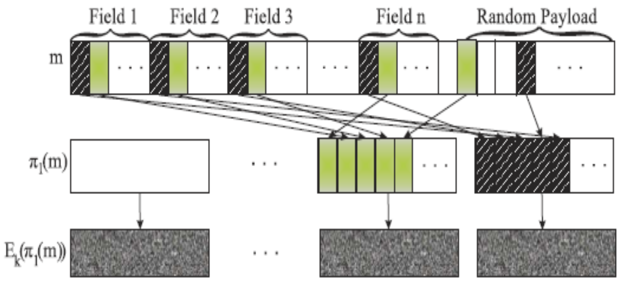

Fig 3

IV.PERORMANCE EVALUATION

We simulated the energy efficient localization technique on Network Simulator (version 2) widely known as NS2 [11], a scalable discrete-event driven simulation tool. Building high performance WSN network systems requires an understanding of the behavior of sensor network and what makes them fast or slow. In addition to the performance analysis, we have also evaluated the proposed technique in measuring, evaluating, and understanding system performance. The final but most important step in our experiment is to analyze the output from the simulation. After the simulation we obtain the trace file which contains the packet dump from the simulation.

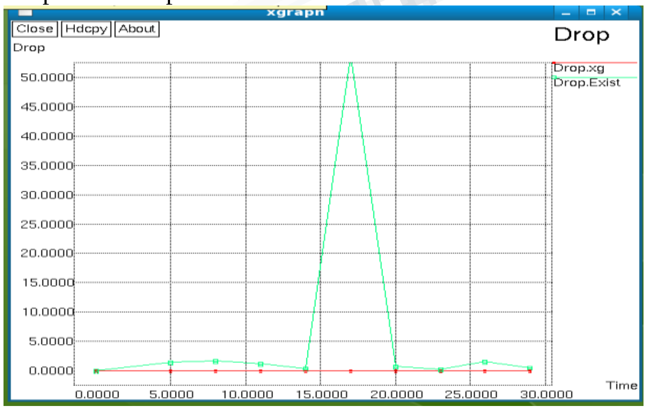

Fig 1 Drop vs Time

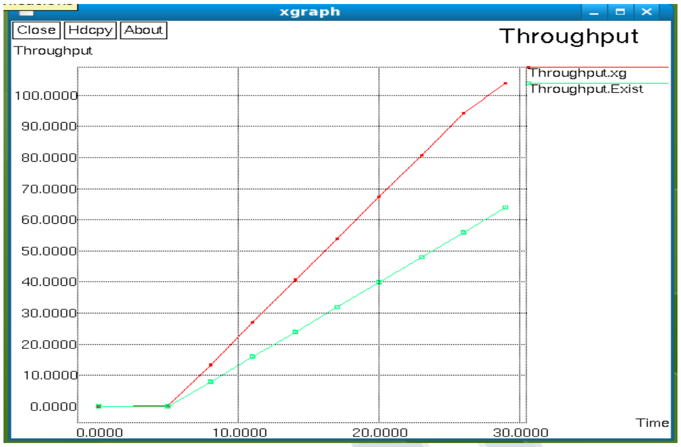

Fig 2 Throughput vs Time

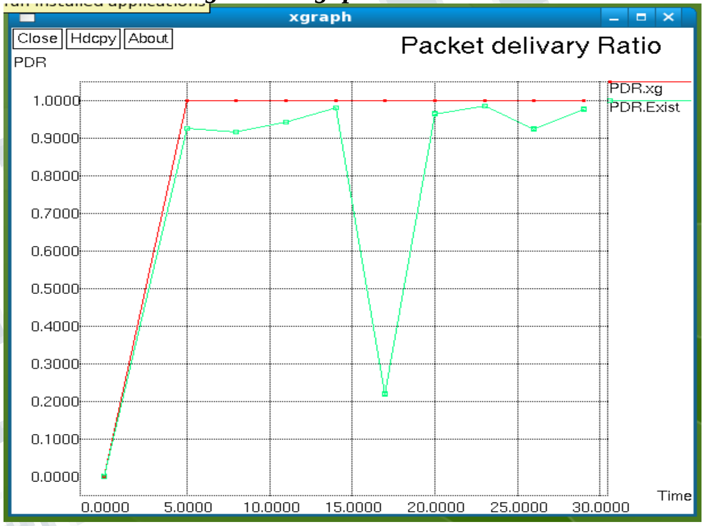

Fig 3 Packet Delivery Ratio vs Time

V. CONCLUSION

After simulating the source and destination formation file on Network Simulator (version 2.32) widely known as NS2, a scalable discrete-event driven simulation tool. Building high performance WSN network systems requires an understanding of the behavior of sensor network and what makes them fast or slow. In addition to the performance analysis, we have also evaluated the proposed technique in measuring, evaluating, and understanding system performance. The final but most important step in our experiment is to analyze the output from the simulation. After the simulation we obtain animation which shows the movement of nodes along with the snake type dynamic movement and various node points. With the help of that we will identify the location of all nodes finally the location details file generated which contains the Source, Destination, SX-Pos, SY-Pos, Distance(d) .

Thus we conclude that the different methods of selective jamming attacks at source and destination nodes were studied and verified the desired output.

REFERENCES

[1] Alejandro Proan˜o and Loukas Lazos, "Packet-Hiding Methods for Preventing Selective Jamming Attacks"
Ieee Transactions On Dependable And Secure Computing, Vol. 9, No. 1, January/February 2012.

[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] M. Cagalj, S. Capkun, and J.-P. Hubaux. Wormholebased antijamming techniques in sensor networks, IEEE Transactions on Mobile Computing, 6(1):100– 114, 2007.

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

[5] 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.

[6] Y. Desmedt. Broadcast anti-jamming systems. Computer Networks, 35(2-3):223–236, February 2001.

[7] K. Gaj and P. Chodowiec. FPGA and ASIC implementations of AES, Cryptographic Engineering, pages 235–294, 2009

[8] O. Goldreich. Foundations of cryptography: Basic applications. Cambridge University Press, 2004
[9] 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

[10] IEEE.IEEE802.11standard. http://standards.ieee.org /getieee802 / download/802.11-2007.pdf, 2007

[11]A. Juels and J. Brainard. Client puzzles: A cryptographic countermeasure against connection depletion attacks. In Proceedings of NDSS, pages 151–165, 1999.

[12]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.

[13] L. Lazos, S. Liu, and M. Krunz. Mitigating controlchannel jamming attacks in multi-channel ad hoc networks, In Proceedings of the 2nd ACM conference on wireless network security, pages 169–180, 2009.

[14] 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.