PACKET-HIDING METHOD TO PREVENT SELECTIVE JAMMING ATTACKS

Prof. Sanjay S.Kulkarni[1], Prof. Atul D.Atalkar [2]

Prof. Anuprita P.Gawande [3]

[12&3] Assistant Professor, Dept.of Electronics & Telecommunication Engg. ,

Shivajirao S. Jondhale College of Engineering & Technology Asangaon (Thane), India.

ABSTRACT:

In this paper, we address the problem of selective jamming attacks in wireless networks. In these attacks, the adversary is active only for a short period of time, selectively targeting messages of high importance. We illustrate the advantages of selective jamming in terms of network performance degradation and adversary effort by presenting two case studies; a selective attack on TCP and one on routing. We show that selective jamming attacks can be launched by performing real-time packet classification at the physical layer. To mitigate these attacks, we develop three schemes that prevent real-time packet classification by combining cryptographic primitives with physical layer attributes. We analyze the security of our methods and evaluate their computational and communication overhead.

1. INTRODUTION

1.1 OVERVIEW

Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes. However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. 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. Typically, 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. However, adopting an "always-on" strategy has several disadvantages. First, the adversary has to expend a significant amount of energy to jam frequency bands of interest. Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect.

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. Potential disclosure of secrets due to node compromise neutralizes the gains of SS. Broadcast communications are particularly vulnerable under an internal threat model because all intended receivers must be aware of the secrets used to protect transmissions.

2.REVIEW OF LITERATURE

Timothy et.al address problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. Jamming is broken down into layers and this paper focuses on jamming at the Transport/Network layer. Jamming at this layer exploits AODV and TCP protocols and is shown to be very effective in simulated

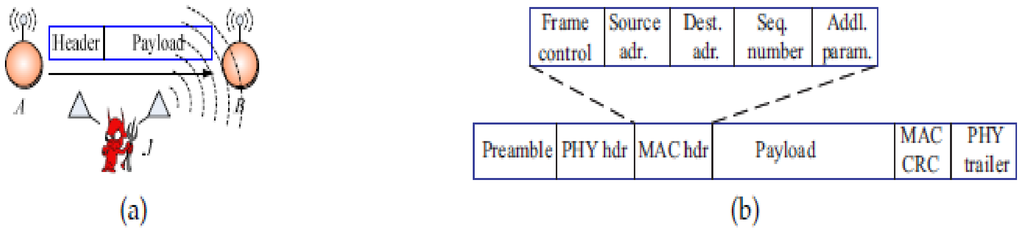
and real networks when it can sense victim packet types, but the encryption is assumed to mask the entire header and contents of the packet so that only packet size, timing, and sequence is available to the attacker for sensing.
M. Cagalj et.al Due to their very nature, wireless sensor networks are probably the most vulnerable category of wireless networks to “radio channel jamming”-based Denial-of-Service (DoS) attacks: An adversary can easily mask the events that the sensor network should detect by stealthily jamming an appropriate subset of the nodes; in this way, he prevents them to report what they are sensing to the network operator.
LoukasLazos et.al addresses the problem of control-channel jamming attacks in multi-channel ad hoc networks. Deviating from the traditional view that sees jamming attacks as physical-layer vulnerability, we consider a sophisticated adversary who exploits knowledge of the protocol mechanics along with cryptographic quantities extracted from compromised nodes to maximize the impact of his attack on higher-layer functions.

3.EXISTING SYSTEM

In Existing System Wireless networks rely on the uninterrupted availability of the wireless medium to interconnect participating nodes.However, the open nature of this medium leaves it vulnerable to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject spurious messages, or jam legitimate ones. While eavesdropping and message injection can be prevented using cryptographic methods, jamming attacks are much harder to counter. They have been shown to actualize severe Denial-of-Service(DoS) attacks against wireless networks.

4.PROPOSED SYSTEM

In this 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 route-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. Selective jamming requires an intimate knowledge of the physical (PHY) layer, as well as of the specifics of upper layers.



(a) (b)

(a) Realization of a selective jamming attack, (b) a generic frame format for a wireless network.

Fig.Realization Of Jamming

4.SYSTEM DESIGN

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.

4.1 SELECTIVE JAMMING AT THE TRANSPORT LAYER

In the first set of experiments, we set up a file transfer of a 3 MB file between two users A and B connected via a multihop route. The TCP protocol was used to reliably transport the requested file. At the MAC layer, the RTS/ CTS mechanism was enabled. The transmission rate was set to 11 Mbps at each link. The jammer was placed within the proximity of one of the intermediate hops of the TCP connection. Four jamming strategies were considered:

1.Selective jamming of cumulative TCP-ACKs.
2.Selective jamming of RTS/CTS messages.
3.Selective jamming of data packets.
4.Random jamming of any packet.

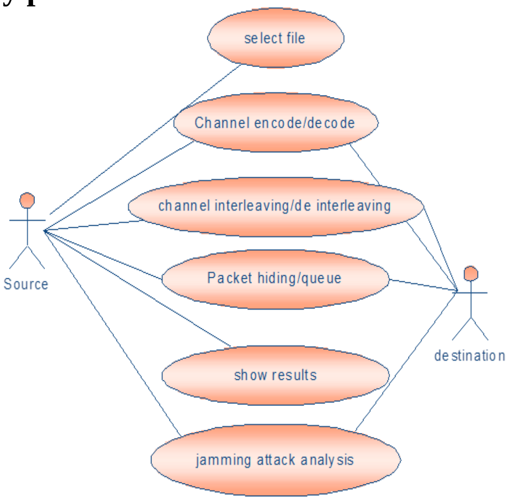


fig .Work Flow

5.IMPLEMENTATION

5.1 DATA FLOW DIAGRAM

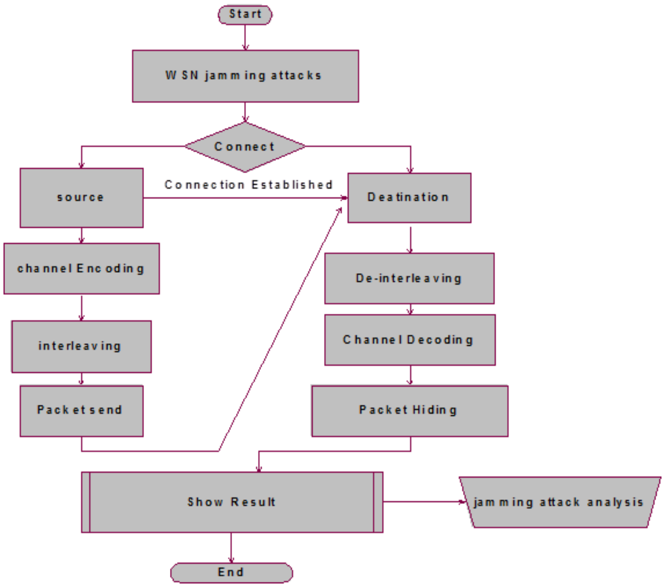
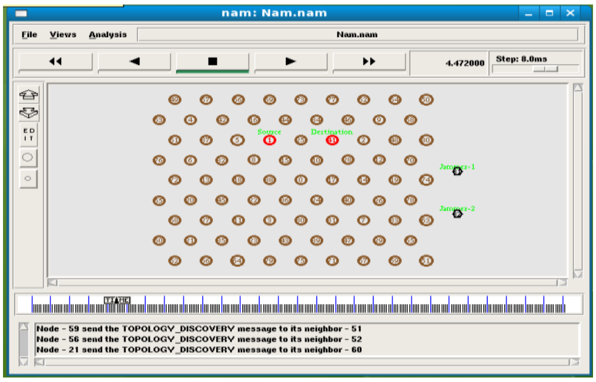
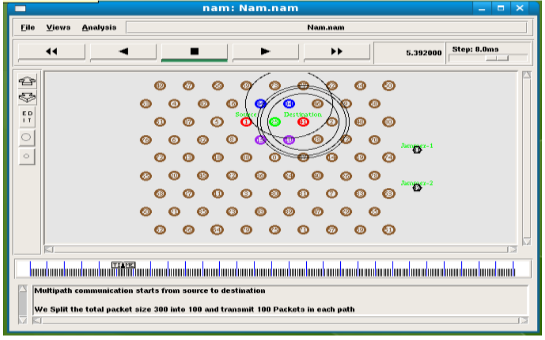


Fig .Data Flow Diagram



Node - 59 send the TOPOLOGY_DISCOVERY message to its neighbor - 51
Node - 56 send the TOPOLOGY_DISCOVERY message to its neighbor - 52
Node - 21 send the TOPOLOGY_DISCOVERY message to its neighbor - 60

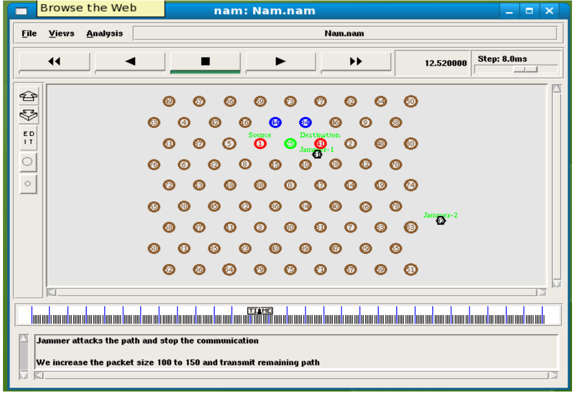
Fig . Source And Destination Formation



Multipath communication starts from source to destination

We Split the total packet size 300 into 100 and transmit 100 Packets in each path

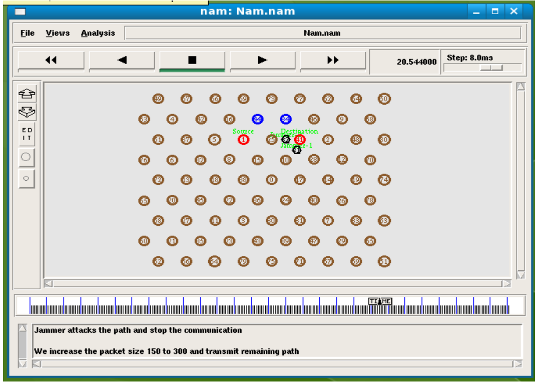
Fig .Mobility Of Nodes



Jammer attacks the path and stop the communication

We increase the packet size 100 to 150 and transmit remaining path

Fig .Jammer 1 Attack

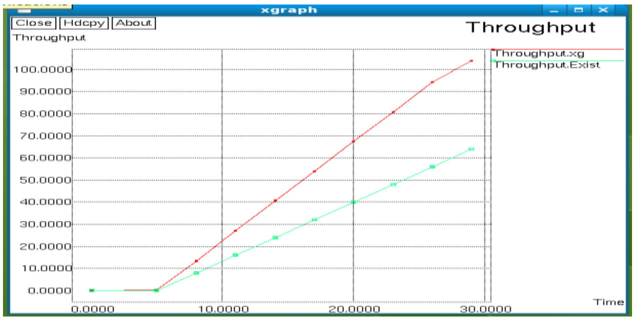


Jammer attacks the path and stop the communication

We increase the packet size 150 to 300 and transmit remaining path

Fig .Jammer 2 Attack

5.2 PERFORMANCE EVALUATION

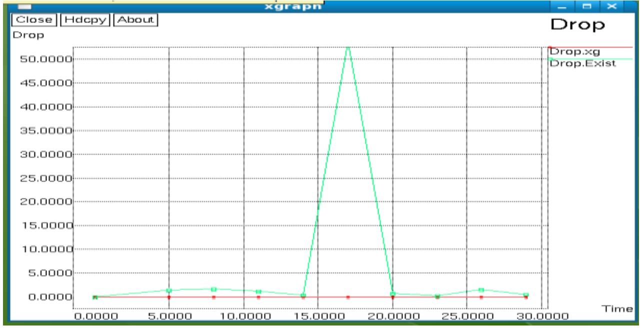


Graph 1.Throughput

Above graph is Throughput vs. Time.

It can be Calculated As

Throughput = File Size / Transmission Time

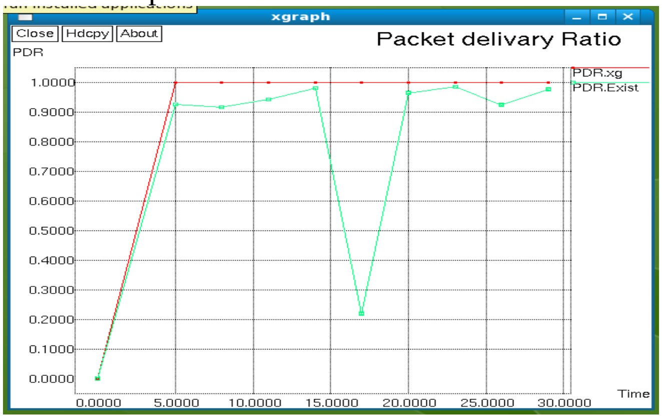


Graph 2.Drop

Above graph Drop vs. Time

It can be calculated as

Drop Time = End Time - Start Time



Graph 3.Packet Delivery Ratio

Above graph is PDR vs. Time

It can be calculated as

PDR = No.of Packet receive at Destination node / No.of packet at Source node

6.CONCLUSION

The goal of this paper was to compare the performance of jamming attacks generated by differing types of jammers, and to compare ad-hoc routing protocols. The conclusions drawn from the research was divided in between three sections.

6.1 JAMMING ATTACKS IN WLANS

The research began from understood the elements that influence the performance of WLANs. Experiments were done in order to demonstrate that distance and power levels from the access points were the main factors that vary the throughput of nodes. The larger the distance between nodes and access points were, the weaker the signal would be. Also, the smaller the power of an access point was, the weaker the signal would be.

Jamming attacks launched by different jammers in WLANs were studied and analyzed. In Scenario 2, a pulse jammer was used in a client-server network. The result proved that jamming attacks did influence the communication between legitimate nodes. When a node traveled toward the pulse jammer, the throughput of the node dropped significantly. The data dropped by the node increased depending on the distance between the node and jammer. The closer the distance was, the more data was dropped. Also, the power level of the jammer varied the performance of the nodes as well. The more powerful a jammer was, the wider the influence would be.

A mobile jammer was utilized in a client-server network. The result of this experiment demonstrated how much jamming attacks can influence a network. The legitimate nodes received fewer packets while the mobile jammer was in close proximity, and communications returned to normal as the jammer traveled out of range.

REFERENCES

[1] AlejandroProan˜o and LoukasLazos, “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.Wormholebasedantijamming 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.