ADVANCED TECHNIQUES FOR PREVENTING SELECTIVE JAMMING ATTACKS

[1]Abhimanyu.V ,[2]L.M.Nithya

M.E. CCE

SNS COLLEGE OF TECHNOLOGY

[1]abhimanyuvvijayan@gmail.com,[2]lmnithya@gmail.com

Abstract

The wireless medium is always subjected to jamming attacks. These Jamming attacks can be used for launching Denial-of-Service attacks on wireless networks. Jamming has been considered as external attack model, but if the attack is internal it cannot be solved by using methods such as spread spectrum methods. In case of internal attacks, the adversary launches jamming attacks in which it targets highly important packets. First the problem of packet classification can be mapped to the hiding property of commitment methods, and propose a packet-hiding method based on commitments in which transmitter and receiver commit on a particular static key. A swarm based vulnerable prevention mechanism based on swarm intelligence is proposed against jamming attacks in wsn. Swarm intelligence algorithm is good in adapting according to change in network topology and traffic. Another method named channel surfing methods using attracting nodes to defend against selective jamming/dropping attacks is also proposed for enhanced security.

Keywords

Channel Surfing Method, , Denial of Service ,Attractingnodes, Selective jamming/dropping Attacks, Swarm Based Vulnerable prevention Mechanism.

1.Introduction

Jamming or dropping attacks are a type of external attack model attacks in which the adversary is not a part of the network. Under this model, jamming methods include the continuous transmission of high-frequency noise signals and attacker can launch low-effort jamming attacks that are difficult to detect and solve. In these attacks, the jammer is active only for a short period of time, selectively aiming messages of high importance. Selective jamming/dropping attacks[1] can be doed by real-time packet classification at the physical layer. To do selective jamming/dropping, the adversary must be capable of classifying transmitted packets in real time, and changing them before the end of their transmission. Packet classification is done by receiving just a few bytes of a packet. To launch selective jamming/dropping attacks, the jammer must be capable of implementing a "classify-then-jam" policy before the completion of a wireless transmission. Jamming attacks are much harder to solve and more security problems. In the simplest form of jamming, the jammer interferes with the reception of messages by transmitting a continuous jamming signal or several short jamming pulses .To mitigate these kinds of attacks, a method that prevent classification of transmitted packets in real time is developed. First the problem of real-time packet classification can be mapped to the hiding property of commitment method, and propose a packet-hiding method based on commitments in which transmitter encrypts a message using a static key and send it to the receiver. The receiver receives the message and decrypt it using the same static key. Another method named swarm based defense mechanism, is proposed which is based on swarm intelligence[5] in which a swarm ants are employed to detect vulnerable channels

and nodes. Another method called attracting nodes is proposed which is based on channel surfing.

2.Existing System

The existing system address the problem of jamming/dropping under an internal adversary model in which the jammer is aware of the implementation details of the network protocols. By utilizing this knowledge, the adversary launches selective jamming/dropping attacks in which it targets specific packets of "high" importance. selective jamming/dropping in terms of network doance degradation and adversary effort by presenting two case studies; The selective jamming/dropping attacks can be launched by doing real-time packet classification at the physical layer. To do selective jamming/dropping, the adversary must be capable of classifying transmitted packets in real time, and changing them before the end of their transmission. Packet classification can be done by receiving a few bytes of a packet. To launch selective jamming/dropping attacks, the jammer must be capable of implementing a "classify-then-jam" policy before the completion of a wireless transmission. Such s can be actualized would by classifying transmitted packets using protocol semantics. Jamming attacks are much harder to solve and have more security problems. They have been shown to cause severe Denial-of-Service (DoS) attacks against wireless networks. In the simplest form of jamming, the jammer interferes with the reception of messages by transmitting a continuous jamming signal .Under this model, jamming methods include the continuous or random transmission of high power interference signals.

3.Proposed System

The proposed method investigates the impact of selective jamming/dropping on critical network functionalities. The findings indicate that selective jamming/dropping attacks lead to a DoS with very low effort on behalf of the jammer. To resolve such attacks, a method that prevent classification of transmitted packets in real time is developed .The problem of real-time packet classification can be mapped to the hiding property of commitment methods in which transmitter and receiver commit on a static key. The transmitter encrypts the message using a private key and the receiver decrypts the message using the same static key. Another method named a swarm based vulnerable prevention mechanism(SBPM) for jamming attacks in wireless sensor networks is proposed which is based on swarm intelligence(SI). Swarm intelligence algorithm is capable enough to adapt change in network topology and traffic. The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The jammers remain on a single channel changing to disrupt any fragment that may be transmitted in the pulse jamming method. Using the swarm based vulnerable prevention method, the forward ants would unicast or broadcast at each node depending on the availability of the channel data for end of the channel. If the channel data is available, the ants randomly choose the next hop. As the checked ants reaches the source, the data collected is checked which channel there is prevalence of adversary long time, and those are omitted. At the same time the forward ants are sent through other channels which are not detected before for attacks.

The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The pair-wise shared key KS is used for creating a channel key KCh = EKS(1) , which generates a pseudorandom channel sequence. Using packet fragmentation method, the packets are break into fragments to be transmitted separately on different channels and with different SFD (start of frame delimiter). The last fragment contains a frame check sequence FCS for the entire payload. The time to transmit the fragment is

If the fragments are short, the adversary's jamming message does not start till the transmitter has finished transmitting and hopped to another channel. In the Pulse Jamming attack, the jammer remains on a single channel ,changing to disrupt any fragment that may be transmitted.

. In future a pre-emptive detection policy using attracting nodes and a response mechanism based on the existing channel surfing algorithm is used to protect wireless nodes from a jammer. Attracting nodes create dummy communication at a frequency close to the actual frequency of operation, so that the real nodes can jump to another frequency even before a jammer starts scanning that frequency.

4.Commitment Methods

Commitments is based on symmetric cryptography. Our main aim is to satisfy the strong hiding characteristics while keeping the computation and communication overhead to a minimum. The proposed SHCS requires the joint consideration of the MAC and PHY layers. To decrease the overhead of SHCS, the de commitment value d (i.e., the decryption key k) is carried in the same packet as the committed value. This helps to save the extra packet header needed for transmitting d individually. To achieve the strong hiding characteristic, a sub layer called

the "concealing sub layer" is inserted between the MAC and the PHY layers. This sub layer is authorized for formatting m before it is processed by the PHY layer. A frame m at the MAC layer delivered to the hiding sub layer. Frame m contains a MAC header and a payload, followed by the trailer containing the CRC code. Initially, m is permuted by applying a publicly known permutation π_1. The purpose of π1 is to randomize the input to the encryption algorithm and delay the reception of critical packet identifiers such as headers. The computation overhead of SHCS is one symmetric encryption at the transmitter and one symmetric decryption at the receiver.

5.Swarm Ants Implementation

A swarm based defense method for jamming attacks in wireless sensor networks is proposed. Swarm intelligence algorithm is capable enough to adapt change in network topology and traffic. The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The jammers remain on a single channel, changing to disrupt any fragment that may be transmitted in the pulse jamming method. Using swarm intelligence mechanism, the forward ants would unicast or broadcast at each node depending on the availability of the channel data for end of the channel.

6. Vulnerable channel Detection

If the data about channel is available, the ants randomly choose a hop. As the checked ants reaches the source, the data collected is checked which channel there is presence of adversary long time, and those channels are omitted. The swarm intelligence method which updates the sensor details more efficiently and successfully. In our proposed work, DEEJAM is combined with swarm method such that swarm's forward and checked ants scan through all the channels in a fast way and detects effectively the jamming activity by informing the legitimate node. Then legitimate node swaps the channel by avoiding the affected channel. This will improve the detection of a jammer quickly with less complication.

The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The pair-wise shared key KS is used for creating a channel key KCh = EKS(1) , which generates a pseudorandom channel sequence. Using packet fragmentation method, the packets are break into fragments to be transmitted separately on different channels and with different SFD (start of frame delimiter). The last fragment contains a frame check sequence FCS for the entire payload. If the fragments are short, the adversary's jamming message does not start till the transmitter has finished transmitting and hopped to another channel.

The advent of wireless networks has brought a new set of security issues with it. The most vulnerable of these is a jamming based attack. This is because with the already existing network architecture, there is nothing that can be done to overcome a jamming attack. In this paper a pre-emptive detection policy using attracting nodes and a response mechanism based on the existing channel surfing algorithm is used to protect wireless nodes from a jammer. Attracting nodes generate duplicate communication at a frequency close to the actual frequency of operation, so that the true nodes can move to another frequency even before a jammer starts scanning that frequency.

7.System Architecture

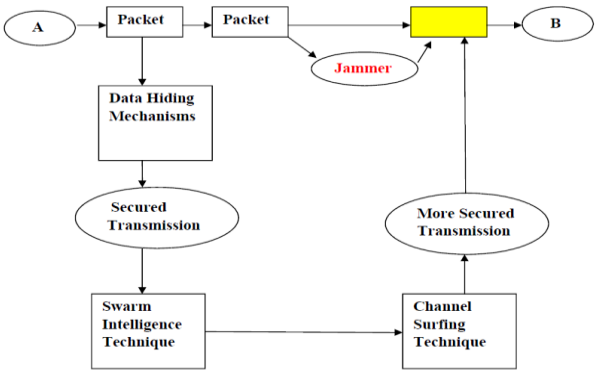

Fig.1. System Architecture of Preventing Mechanism

8.Results

Network Simulator,NS2 is used to simulate the proposed architecture NS2 is a discrete event simulator targeted at networking research developed by Uc Berkely.NS2 is written in C+ + and Otcl. NS2 provides support for simulation of TCP and multicast protocols over wired and wireless networks.

In the simulation a wireless sensor network employed with six nodes including a jammer is used. By using the advanced methods we chow that average throughput and delivery ratio has improved considerably.

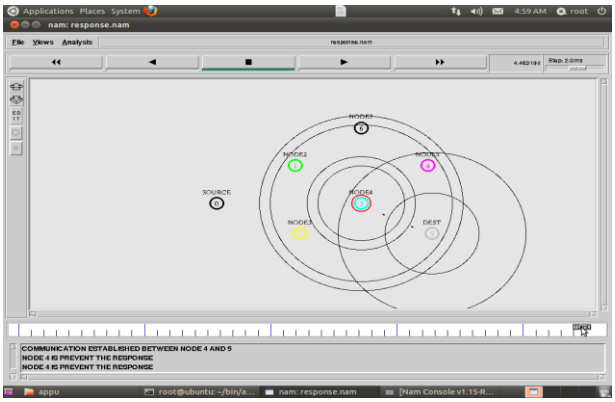

Fig.2.Snapshot of NS2 Simulator Output

9.Conclusion

The selective jamming/dropping attacks can be launched by performing real-time packet classification at the physical layer. The proposed method investigates the impact of selective jamming/dropping on critical network functions and develops three methods that prevent classification of transmitted packets in real time. First the problem of real-time packet classification can be mapped to the hiding property of commitment methods and propose a packet-hiding method based on commitments. Second a packet-hiding method based on cryptographic puzzles. Finally All -or- Nothing Transformations that introduces a modest communication and computation overhead .A swarm based vulnerable prevention mechanism for jamming attacks in wireless sensor networks. Finally the swarm intelligence method which updates the sensor details more efficiently and successfully. This swarm based defense method for jamming attack is most effective. Using social insect metaphor for solving various problems is the main basis of swarm intelligence. Ants, bees, and termites are the insects which live in colonies. Every insect in colony have their own plans.

In our enhanced approach, swarm based vulnerable prevention mechanism for jamming attacks in wireless sensor networks . Swarm intelligence algorithm is capable enough to adapt change in network topology and traffic. The transmitter and receiver change channels in order to stay away from the jammer, in channel changing method. The jammers remain on a single channel changing to disrupt any fragment that may be transmitted in the pulse jamming method. Using the swarm based vulnerable prevention method, the forward ants would unicast or broadcast at each node depending on the availability of the channel data for end of the channel. If the channel data is available, the ants randomly chooses a hop. As the checked ants reaches the source, the data collected is checked which channel there is presence of adversary long time, and those are omitted. At the same time the forward ants are sent through other channels which are not detected before for attacks. This method helps reduce the channel maintenance overhead.

A pre-emptive detection policy using attracting nodes and a response mechanism based on the existing channel surfing algorithm is used to protect wireless nodes from a jammer. Attracting nodes generate duplicate communication at a frequency close to the actual frequency of operation, so that the real nodes can jump to another frequency even before a jammer starts scanning that frequency.

10.References

[1] *Alejandro Proano And Loukas Lazos January/February 2012 "Packet Hiding Methods for Preventing Selective jamming/dropping Attacks"IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING (vol. 9 no. 1)*

[2] *Lookas Lazos and Marwan Krunz February 2012 "Selective jamming/dropping/Dropping Insider Attacks in Wireless Mesh Networks" IEEE NETWORK Volume:25 Issue:4*

[3] *Wenyuan Xu, Timothy Wood, Wade Trappe, Yanyong Zhang 2004"Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service" WiSe '04 Proceedings of the 3rd ACM workshop on Wireless security Pages 80 - 89 ACM New York, NY, USA*

[4] *Wenyuan Xu, Wade Trappe, Yanyong Zhang and Timothy Wood 2005"The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks" MobiHoc '05 Proceedings of the 6th ACM international symposium on Mobile ad hoc networking and computing*

[5] *S.Periyanayagi and V.Sumathi December 2011"A Swarm Based Defense Method for Jamming Attacks in Wireless Sensor Networks" International Journal of Computer Theory and Engineering, Vol. 3, No. 6*

[6] *Sudip Misra,Sanjay.K.Dhurander,Avanish Rayankula and Deepansh Agarwal 26-31 Oct. 2008 "Using Honeynodes along with Channel Surfing for Defense against Jamming Attacks in Wireless Networks"3rd International Conference on System and Network Communications Page-197-201*

[7] *Shio Kumar Singh , M P Singh , and D K Singh May to June Issue 2011 " A Survey on Network Security and Attack Defense Mechanism For Wireless Sensor Networks" International Journal of Computer Trends and Technology"Volume 1*

[8] *Yee Wai Law,Marimuthu Palaniswami,Pieter Hartel,Paul Havinga,Jeroen Doemen and Lodewijk Van Hoesel February 2009 "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols" ACM Transactions on Sensor Networks (TOSN) Volume 5 Issue 1*

[9] *Timothy X Brown,Jesse .E.James and Amitha Sethi 2006"Jamming and Sensing of Encrypted Wireless Ad Hoc Networks" MobiHoc '06 Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing Pages 120-130*

[10] *Agnes Chan,Xin Liu,Guevara ,Bishal Thapa 2007 "Control Channel Jamming: Resilience and Identification of Traitors" IEEE International Symposium on Information Theory (ISIT)*

[11] *Wenyuan Xu,Wade Trappe and Yanyong Zhang May-June 2006 "Jamming Sensor Networks:Attack and Defence Strategies"IEEE Networks*

[12] *Tian Fu "Modelling and Simulation of Jamming nodes in WLAN"April 2012 http://thescholarship.ecu.edu/bitstream/handle/10342/3888/Fu_ecu_0600M_10649.pdf?sequence=1*

[13] *Loukas Lazos, Sisi Liu and Marwan Krunz 2009 "Mitigating control-channel jamming attacks in multi-channel ad hoc networks" WiSec '09 Proceedings of the second ACM conference on Wireless network security Pages 169-180*

[14] *Yee Wai Law,Marimuthu Palaniswami,Pieter Hartel,Paul Havinga,Jeroen Doemen and Lodewijk Van Hoesel February 2009 "Energy-Efficient Link-Layer Jamming Attacks against Wireless Sensor Network MAC Protocols" ACM Transactions on Senser Networks(TOSN),Volume 5,Issue 1*

[15] *Timothy X Brown,Jesse .E.James and Amitha Sethi 2006 "Jamming and Sensing of Encrypted Wireless Ad Hoc Networks" MobiHoc '06 Proceedings of the 7th ACM international symposium on Mobile ad hoc networking and computing Pages 120-130*

[16] *Aristides Mpitziopoulos and Damianos Gavalos 2008"An effective defence node against jamming attacks in sensor networks" SECURITY AND COMMUNICATION NETWORKS Security Comm. Networks.Published online in Wiley InterScience(www.interscience.wiley.com) DOI: 10.1002/sec.81*

[17] *Mario Cajalg,Srdjun Capkun and Jean-Pierre Hubaux JANUARY 2007 "Wormhole based antijamming methods in Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 6, NO. 1*

[18] *Miroslav Pajic and Rahul Mangharam September 2008. "Wispernet:Anti jamming for Wireless Sensor Networks" University of Pennsylvania Scholarly Commons 2nd Workshop on Embedded Systems Security (WESS'08), IEEE/ACM EMSOFT '08 and the Embedded Systems Week*

[19] *Alexandros G. Fragkiadakis, Vasilios A. Siris,Apostolos P. Traganitis 2010 "Effective and Robust Detection of Jamming Attacks" Future Network and Mobile Summit 2010 Conference Proceedings Paul Cunningham and Miriam Cunningham (Eds)IIMC International Information Management Corporation, 2010 ISBN: 978-1-905824-18-2*

[20] *Yalin Evren Sagduyu, Randall A. Berryy, and Anthony Ephremidesz May-June 2010 "Wireless Jamming Attacks under Dynamic Traffic Uncertainty"Modelling and Optimization in Mobile Adhoc and Wireless Networks(WiOpnet) pages 303-312*

[21] *Mika Stahlberg "Radio Jamming Attacks Against Two Popular Mobile Networks"2008 Helsinki University of Technology Seminar on Network Security.*

[22] *Hoang Nguyen, Thadpong Pongthawornkamol and Klara Nahrstedt 2011 "Alibi: A framework for identifying insider-based jamming attacks in multi-channel wireless networks" Global TeleCommunication Conference(GLOBECOM 2011) IEEE*

[23] *Mingyan Li,Iordanis Koutsopoulos, Radha Poovendran August 2010 "Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks"IEEE Transactions on Mobile Computing*

[24] *Mithun Acharya, David Thuente "Intelligent Jamming Attacks, Solveattacks in 802.11b Wireless Networks"*

[25] *Arif Sari and Dr. Beran Necat June 2012 "Securing Mobile Ad-hoc Networks Against Jamming Attacks Through Unified Security Mechanism" International Journal of Ad hoc, Sensor & Ubiquitous Computing (IJASUC) Vol.3, No.3*