Available online at www.elixirpublishers.com (Elixir International Journal)

Information Technology

Elixir Inform. Tech. 76 (2014) 28705-28708

ISSN: 2229-712X

A review prevention of jamming attacks in wireless network using internal threat model

Vivek N. Waghmare, Vaishali D. Borade and Arpita P. Biswas

Information Technology Department, Sandip Institute of Technology & Research Center, Nasik, India.

ARTICLE INFO

Article history:

Received: 22 September 2014;

Received in revised form:

10 November 2014;

Accepted: 21 November 2014;

Keywords

AODV, TCP, DoS,

Eaves dropping.

ABSTRACT

In a network multiple clients sends multiple messages from multiple computers to one computer at the same time, the problem of jamming occurs at the intermediate node, So that the opponents can easily target the messages of high importance. Opponents are able to retrieve the data from the messages. This problem is overcome by using the cryptographic primitives to prevent jamming attacks. In internal threat model, RSA algorithm provides security to message transmission over the network. The schemes to prevent jamming attacks such as Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), and All-Or-Nothing Transformation Hiding Schemes (AONTSHS).

Introduction

The accessible nature of wireless medium leaves an intentional interference attack, typically called as jamming [1]. This intentional interference with wireless transmission launch pad for mounting Denial-Of- Service attack on wireless networks [9].Generally, jamming has been addresses under an external threat model. Nevertheless, opponents with internal knowledge of protocol specification and network secrets can launch low effort jamming attacks that are difficult to detect and counter. In this approach the problem of jamming attacks and adversary is active for less time, selectively targeting the messages of great importance [9]. The jamming attacks can be launched by performing real-time packet classification at the physical layer. To reduce these attacks, three schemes that prevent real time packet classification by combining cryptographic primitives with physical-layer attribute. The schemes are Strong Hiding Commitment Schemes (SHCS), Cryptographic Puzzles Hiding Schemes (CPHS), and All- Or-Nothing Transformation Hiding Schemes (AONTSHS) [9]. Random key classification methods are done along with three schemes to give using cryptographic methods; jamming attacks are more difficult to counter .Jamming attacks have been shown to realise severe Denial-of-Service (DoS) attacks against wireless networks. In the lowest form of jamming, the opponent interferes with the reception of messages by transmitting a continuous jamming signal, or several short jamming pulses [1]. Jamming attacks have been considered under an external threat model, in which the jammer is not component of the network. In this model, jamming strategies include the continuous or random transmission of high power interference signals. Nevertheless, adopting an al- ways-on method has several drawbacks. First, the opponent has to consume a significant amount of energy to jam frequency bands.

Second, the continuous presence of unusually high interference levels makes this type of attacks easy to detect. Anti-jamming techniques extensively on spread spectrum communications, or some form of jamming shift. The spread spectrum techniques gives bit-level security by scattering bits according to a secret pseudo noise (PN) code, Known only to the sender and receiver. These techniques can only secure wireless transmissions in the external threat model [1]. Potential disclosure of secrets neutralizes the gains of SS due to node settlement. Broadcast communications are helpless in an internal threat model due to all intended receivers who must be aware of the secrets used to secure transmissions. Therefore, the settlement of a single receiver is enough to reveal relevant cryptographic information. Jamming problem is solved using an internal threat model. Consider a opponent of network protocols at any layer in the network. The opponent achieves his internal knowledge for launching selective jamming attacks in which particular 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 reduce the throughput of an end-to end flow. Wireless networks depend on the uninterrupted availability of the wireless medium to interconnect participating nodes. The accessible nature of this medium leaves it harmful to multiple security threats. Anyone with a transceiver can eavesdrop on wireless transmissions, inject fake messages, or jam legal ones. While eaves-dropping and message injection can be avoided. Wireless networks now enjoy extensive commercial Implementation due to their low cost, ease of use and setup. Since accessing wireless media is much comfortable than tapping a wired network, security becomes a serious concern when implementing any wireless network. Consider a particular class of Denial of Service (DoS) attacks called jamming [1]. Jamming results in a loss of link reliability, increment energy consumption, extended packet delays and disruption of end-to-end routes. The use of different, dedicated communication channels to transmit data and control traffic introduces a single point of failure for a denial of service Attack, in that an opponent may capable to jam control channel traffic and prevent current data traffic. Jamming techniques in the external threat model involves the continuous or random transmission of high power interference signals [2]. Along the knowledge of network protocols, the opponent goal the specific packets of high priority by launching jamming attack. The adversary must be able to classify transmitted packets in real time, and corrupting them before the end of their transmission,

Tele:

E-mail addresses: vaishaliborade925@gmail.com

to perform jamming. Packet classification can be performed by receiving just a few bytes of a packet [1].

Related Work

In related work the reasons of jamming, how it will take place, how it will work are described. Spread spectrum technique is used by conventional anti-jamming methods [2]. Because of jamming wireless transmission is either stopped or disturbed. The jamming is either in the form of interference, noise or collision. If the jamming is intentionally then it is in the form of attack otherwise it is caused because of network traffic [4]. It doesn't require any special hardware for execution. Anti-jamming methods are based on either some form of jamming shift or SS communications. First the input is given to channel encoder, then the channel encoder creates analog signal which consist of narrow bandwidth [3]. This created signal is modulated by using the sequence of digits. Pseudo noise or pseudo-random number generator is the main source for creating the Spreading code [2]. The main purpose of using modulation mechanism is to increase signal's bandwidth which is going to be transmitted [13]. This whole procedure is carried at the sender side. Now at the receiver side for demodulating the spread spectrum signal digital sequence is used [2]. This generated signal is given to channel decoder in order to recover the original data. Spread spectrum is generally used for hiding and encrypting signals [2].

The wireless networks are usually preferred due to its effective features such as its faster accessibility, compatibility and its connectivity among various users. Because of its better transfer rate the authentication mechanism is ignored in wireless sensor network. This shortens the limitation of the existing wired network. While using the wireless sensor network various types of jamming attacks are invited. Some detection strategies are present but they are failed sometime in analyzing and reporting the presence of jammer. In the external threat model it is little easy but in the internal threat model the person has great knowledge about network secrets and internal protocol specifications. To protect the packets from such attacks packet hiding scheme is implemented []. The in building or campus-wide wireless LANs, network administrators provision cellular resources over long time scales (weeks or months). In bad situations where access points (APs) are able to dynamically pick their operating channels from a wide-band selection, they pick a fixed-width channel in which to operate [14]. The result is that an AP or a cellular base station uses a fixed chunk of the spectrum whenever it transmits, as does a client within a given cell. This fixed-width allocation causes significant throughput problems due to congestion on the wireless medium. These problems have been identified at individual 802.11 hotspots and at sites with multiple access point [14].

LAN provides to users the mobility to move around within a local area without a wire and still connect to the network; it is widely used in many important areas [14]. Banks, governments, corporations, and institutions transmit highly important data through WLANs. The security problems of WLANs become important for the users. Many WLANs are based on the IEEE 802.11 standard, which transmits data in different channels based on frequencies. Because of the ease of installation and convenience, WLAN is regularly used in daily life. WLAN was introduced by Gast (2005) and Mark (2005). Due to the popularity of WLANs, security research must be done in various types of WLANs [13]. The DoS attacks on the physical layer were analyzed and expanded to the security of the physical layer of the sensor network model. By using Receiver Operating Characteristics (ROC) on nodes, attacks can be predicted by formulating the classification of jammers in various attack scenarios. This approach can help improving detecting DoS attacks in WLANs. This approach focuses on two types of WLANs: client-server and ad-hoc networks [13]. The DNS is a hierarchical tree structure whose root node is known as the root domain [4]. The name of label is directly proportional to a node in the DNS tree structure. A label is an alphanumeric string that uniquely identifies that node from other nodes. Labels are connected together with a dot notation, ".", and a DNS name containing multiple labels represents its path along the tree to the root [5]. WLANs are built upon a shared medium that makes it easy to launch jamming attacks. These attacks can be easily accomplished by sending radio frequency signals that do not follow any MAC protocols [1]. Detection of jamming attacks can be done in multiple ways. One of the most efficient ways is to jump channels. Because communication between two legitimate nodes is done with a specific frequency, the frequency can be changed if necessary. While a jammer is attacking the wireless network, there are other effective ways to continue legitimate communication in the network. When the nodes detected the jamming in the wireless network, they jumped to another channel to continue legitimate communication. The channel jumping will decrease the throughput of the network [2]. Also, it is easier to detect jamming through intermitted channel jumping. The channel jumping was a superior method of struggling network interference, rather than changing network protocols. In order to prevent from multi-channel jamming attacks, a cross-layer jamming detection method was developed. Cross-layer jamming detection is a tree-based approach [1]. A jamming detection algorithm was utilized in all legitimate nodes; when the communication process began, all the nodes had the ability to report jamming attacks in different layers, and only the reports which were generated by nodes with jamming detection algorithm were accepted by the system in order to avoid error. The difference from the jamming detection algorithm was that it focused on network restoration and design of traffic rerouting [13].

The simulation and experimental results show that jamming has the potential for large gains, if the packet types are identified. There are two approaches to classifying packets into types. The first classifies packets as they arrive [5]. Jamming can get significant jamming gains, well over 100, when it knows the packet type and timing. Most of these gains were produced by attacking packets above the ad hoc network layer. The Protocols introduce highly predictable timing that can be exploited. The limited information of packet size, timing, and sequence is enough to accurately predict packet types. In future it will fully connect and test the jamming and sensing which were treated separately [5]. The statistical sensing tools continue to be refined. A few representative attacks were presented and the test bed tools described here are being used to methodically evaluate other attacks. The long term goal is scaling to larger ad hoc networks and networked attackers. The problem of control-channel jamming attacks in multi-channel ad hoc networks. The deviated from the traditional view that sees jamming attacks as physical-layer vulnerability. 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 function [11]. There are many different scenarios where a jamming style DoS may take place, but the three basic classes of wireless networks are important. First is Two-Party Radio Communication. The second is the two-party scenario is the baseline case in which A

and B communicates with each other on a specific channel [5]. The transmission will interfere with the transmission and reception of packets by A and B as long as interferer X is close enough to either A or B. The third one is Infrastructure Wireless Networks. The Infrastructure wireless networks consist cellular networks or wireless local area networks (WLANs), it consists of two main types of devices: access points and mobile devices. All the access points are connected to each other by separate and wired infrastructure. The mobile devices communicate by the access point in order to communicate with each other or the Internet. Due to the presence of an interferer might make it impossible for nodes to communicate with their access point [5]. This system describes that How to enable robust anti-jamming broadcast without shared secret keys. Mostly broadcast applications share the need for authenticity and availability of messages that are transmitted by base stations to a large and unknown number of potentially untrusted receivers.

Advantages of Spread Spectrum Technique:

1. It is easy to realize by exploiting knowledge of network protocols and cryptographic primitives extracted from compromised nodes [11].
2. This technique helps to reduce jamming attacks lead to a (DoS) with very low effort on behalf of the jammer [2].
3. It has Strong Security properties.
4. It gives privacy due to the unknown random code.
5. It is capable to eliminate the effects of multipath interference.

Limitations of Spread Spectrum Technique:

1. Broadcast communications are harmful in an internal threat model due to all intended receivers must have the knowledge of the secrets used to secure transmissions.
2. Bandwidth is inefficient.
3. Implementation is little bit complex.

Advantages of Packet Hiding Technique:

1. Wireless networks depend on the uninterrupted availability of the wireless medium to interconnect involved nodes.
2. Data hiding is easy.

Limitations of Packet Hiding Technique:

1. Packet cannot be retrieved easily.
2. It requires more time.

Proposed System

There are many techniques for prevention of jamming attacks in wireless network. One of them is packet hiding technique. This system is based on packet hiding scheme but there are some modifications in this method. Packet hiding method requires jammer compulsory. In packet hiding method there is no secret transmission. These problems are overcome under the internal threat model. This proposed approach describes the architecture of jamming attacks in wireless network. If there are two nodes in network i.e. node A node B. In any network problem of jamming occurs. While sending multiple messages from multiple computers to one computer at the same time jamming occurs on the node so any adversary who knows about network secrets target the messages of high importance and retrieves some information from those messages. This architecture prevents the jamming attacks by using cryptographic primitives. It also uses the encryption and decryption algorithms. In this system the all data will be stored on server side. The intermediate node helps to prevent these types of attacks. This approach uses different methods for the prevention of jamming attacks like strong hiding commitment scheme, all or nothing transmission scheme.

In this system the jamming is prevented by using different techniques. For secure and secret transmission of message it uses the different encryption decryption algorithms. RSA is one of the important algorithms for security of data transmission.

This approach works on following methods:

1) Strong hiding commitment scheme
2) Cryptographic puzzle hiding scheme
3) An AONT-Based Hiding Scheme
4) Real time packet classification
5) RSA algorithm

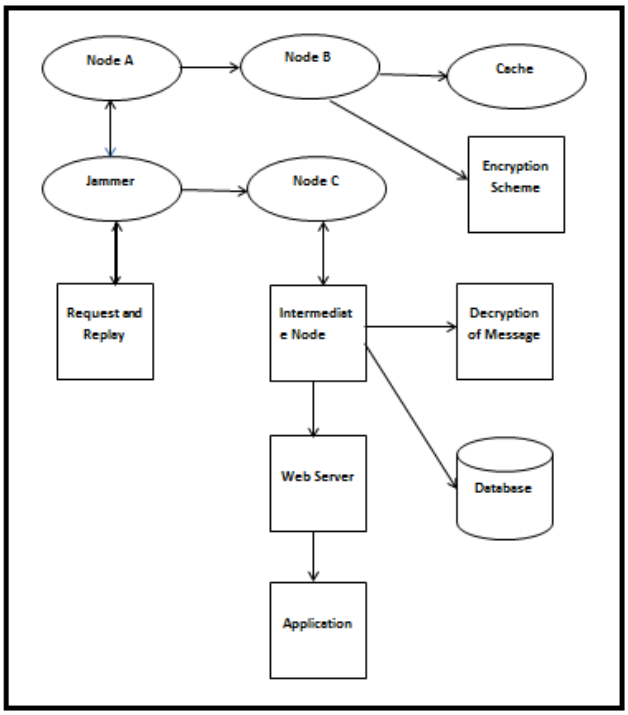

Fig. System Architecture

Strong Hiding Commitment Scheme [11]:

A solution to the jamming attack in the wireless network would be the encryption of packet that is going to send. This is scheme is based on symmetric cryptography. The main reason is to satisfy the strong hiding property while keeping the computation and communication overhead to a minimum. Consider that the sender has a packet for Receiver. First, Sender sends a message to the obligation function is an off-the-shelf symmetric encryption algorithm is a publicly known permutation, and k is a randomly selected key of some desired key length. Then the real message is hided with the help of encryption. Receiver receives the real message which was send by the sender. With the help of scheme the secure data transmission is carried out. Opponents are not able to retrieve the data.

Cryptographic puzzle hiding scheme [11]:

A packet-hiding method is based on cryptographic puzzles. The main purpose behind such puzzles is to force the recipient of a puzzle execute a predefined 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.

An AONT-Based Hiding Scheme [6]:

A solution to prevent jamming attack is based on all-or Nothing Transformations that introduces a modest communication and computation overhead.

Real time packet classification [11]:

In this method the opponent can classify packets in real time, before the packet transmission is completed. Once a packet is classified, the opponent may choose to jam it depending on his techniques. At the PHY layer, a packet m is encoded, allocated, and modulated before it is transmitted over the wireless network. At the receiver, the signal is demodulated, de-allocated, and decoded to recover the original packet m.

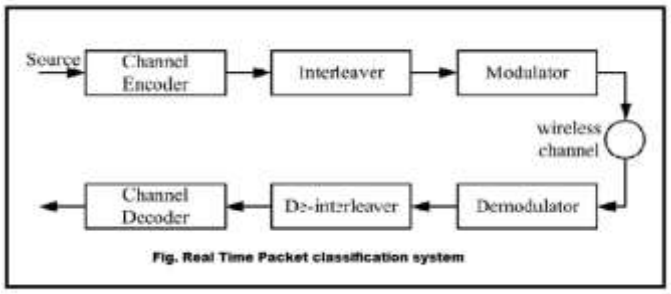

Fig. Real Time Packet classification system

RSA algorithm [5]:

RSA is an Internet encryption and authentication system that uses an algorithm. The RSA algorithm was developed in 1977 by Ron Rivets, Adi Shamir, and Leonard Adelman at MIT. The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape. The encryption system is owned by RSA Security. This algorithm is more secure than other algorithms.

Conclusion:

The problem of jamming attacks in wireless networks has considered an internal opponent model in which the jammer is part of the network under attack. Therefore being aware of the protocol specifications and shared network secrets. The schemes such as commitment schemes, cryptographic puzzles, and all-or-nothing transformations with physical layer characteristics analyses the security of schemes and quantified their computational and communication overhead.

Acknowledgment

We take this opportunity to express my kindness and deep regards to my guide Prof. Vivek N. Waghmare for his guidance, monitoring and constant encouragement throughout the course of this project. The blessing, help and guidance given by him time to time shall carry us a long way in the journey of life.

We are thankful to our project guide Prof. Vivek N. Waghm are and project co-ordinator Prof Vijay R. Sonavane for the valuable information provided by them in their respective fields. We are grateful for their cooperation during the period of our project.

Lastly, we thank almighty, our parents, brother, sisters and friends for their constant encouragement without which this assignment would not be possible.

References:

[1] T.X. Brown, J.E. James, and A. Sethi, Jamming and Sensing of Encrypted Wireless
Ad Hoc Networks, Proc. ACM Intl Symp. Mobile Ad Hoc Networking and Computing (MobiHoc), pp. 120-130,2006.

[2] M. Cagalj, S. Capkun, and J. P. Hubaux,Wormhole-Based Anti- Jamming Techniques in Sensor Networks, IEEE Trans. Mobile Computing, vol. 6, no. 1, pp. 100-114,Jan.2007.

[3] A. Chan, X. Liu, G. Noubir, and B. Thapa, Control Channel Jamming: Resilience and Identification of Traitors, Proc. IEEE Intl Symp. Information Theory (ISIT), 2007.

[4] W. Xu, W. Trappe and Y. Zhang, Anti- Jamming Timing Channels for Wireless Networks, Proc. ACM Conf . Wireless Network Security (WiSec), pp. 203-213, 2008.

[5] Ms. Sonam Choubey, "A Cryptography Based Method for Preventing Selective Jamming Attack in Wireless Network",2014

[6] R. Rivest, All-or-Nothing Encryption and the Package Transform, P roc . International Workshop Fast Software Encryption, pp. 210- 218,1997.

[7] R. Rivest, A. Shamir, and D . Wagner, Time Lock Puzzles and Timed-Release Crypto, technical report, Massachusetts Inst. of Technology, 1996.

[8] P. Tague, M. Li, and R. Poovendran, Mitigation of Control Channel Jamming under
Node Capture Attacks, IEEE Trans. Mobile Computing, vol. 8, no. 9, pp. 1221- 1234, Sept. 2009.

[9] A. Juels and J. Brainard, Client Puzzles: A Cryptographic Countermeasure against Connection Depletion Attacks, Proc. Network and Distributed System Security Symp. (NDSS), pp. 151-165, 1999.

[10] Bharath J and Mr. Rajashekar S A,"SHCS Technique Defined for Packet Hiding Methods in Wireless Networks", March 2013.

[11] Ngangbam Herojit Singh and A.Kayalvizhi, "Combining Cryptographic Primitives to Prevent Jamming Attacks in Wireless Networks",2010.

[12] O.S.C Kesavulu,B.B.V. Satya Vara Prasad and Y. Srinivasa Rao,"Enhanced Packet Delivery Techniques Using Crypto-Logic Riddle on Jamming Attacks for Wireless Communication Medium",4 July 2013.

[13] Katkar Kiran B., Dukare Ajay B., Pawar Monali R. "Survey on Packet Hiding Scheme for Network Security by Selective Jamming Attacks",2014

[14] Ramakrishna Gummadi and Hari Balakrishnan , "Wireless Networks Should Spread Spectrum Based On Demands", 2007.

[15] P. Bahl, R. Chandra, and J. Dunagan. SSCH: Slotted seeded channel hopping for capacity improvement in IEEE 802.11 ad-hoc wireless networks. In *Mobi-Com'04*.

[16] P. Bahl, M. T. Hajiaghayi et al. Cell breathing in wireless LANs: Algorithms and evaluation. *IEEE TMC*, 6 (2), 2007.

[17] A. Balachandran, G.M. Voelker, P. Bahl, and P. V. Rangan. Characterizing user behavior and network performance in a public wireless lan. In *SIGMETRICS'02*.

[18] R. Gallager. "A perspective on multiaccess channels". *IEEE Transactions on Information Theory*, 31(2), Mar 1985.

[19] R. Gummadi, R. Patra, H. Balakrishnan, and E. Brewer. "Interference avoidance and control". In *HotNets'08*