SELECTIVE JAMMING ATTACK PREVENTION BASED ON PACKET HIDING METHODS AND WORMHOLES

Divya Ann Luke, Dr. Jayasudha. J .S

Department of Computer Science and Engineering
SCT College of Engineering, Trivandrum.

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 main attack present in the wireless network is the selective jamming attack. This type of attack mainly focuses a single node termed as target node. Attacker always tries to block the message sent by the target node. This leads to the Denial-of-Service attack. We are proposing a new method to prevent the selective jamming attack in an internal threat model.*

A wormhole is used, which will generate an alarm to indicate the presence of jammer and sent IP address of jammer node to all other nodes in the network. Using a method called packet hiding, we can send message through the network even though a jammer is present. This method is based on the technique called Strong Hiding Commitment Scheme (SHCS). Here, the access point in a network region becomes the wormhole whenever it finds out any node that violates the rules in a particular network region. That node is then considered as a jammer node. The wormhole sends IP address of jammer to all other nodes. Wormhole then prevents the jamming activity of the jammer by encrypting the source ID of message along with the message packet.So that the jammer is unable to identify its target node and the source can forward its message safely through jammer node itself.

KEYWORDS*-Selective jamming, Spread spectrum,Denial-of-Service attack,Wormholes, AES*

1. INTRODUCTION

The wireless networks are more sensitive to the Denial-of-Service (DoS) attacks [1]. In almost every case, jamming causes a denial of service type attack to either sender or receiver. The easiest form of jamming a wireless network communication is to continually transmit useless data to the node where the server becomes overloaded. Most people have no idea if a jamming signal is in use.

It appears as if there is no service.This attack makes the network resource unavailable to its legitimate users. The existing system is based on Spread Spectrum (SS). This technique mainly focused on an external threat model. In broadcast communication, if an attacker present within the network can easily eavesdrop the message sent by any node. In selective jamming attack, the attacker always tries to block the message sent by its target node and it leads to the Denial-of-Service attack [1] [2].

DOI : 10.5121/ijnsa.2014.6308

In this paper, main focus is to prevent selective jamming attack in an internal threat model. A wormhole[3] is used to generate an alarm to indicate the presence of jammer to all access point in the network. Presence of any jammer is detected a method called packet hiding [4] is used to transmit message through the network.

This method is based on the technique called Strong Hiding Commitment Scheme(SHCS) [4]. Alejandro Proano and LoukasLazos [4] proposed a paper based on this technique. Wormhole based anti-jammingconcept along is included in the newly proposed method for eliminating DoS attack.

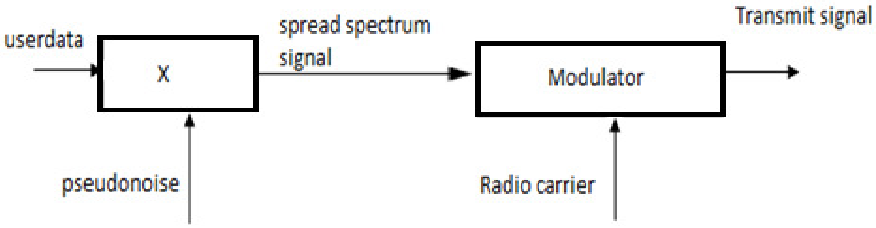

Figure 1. Spread spectrum transmitter

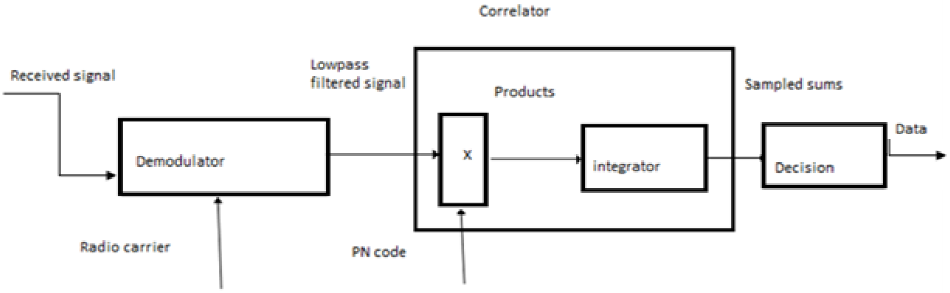

Figure 2.Spread Spectrum receiver

The rest of the paper is organized as follows: Section 2 presents the problem statements, which describes the details about existing system and its disadvantages. Section 3 presents the details about proposed system. Section 4 and 5 describe about the implementation details and performance analysis. Conclusion and directions for future work are given in section 6.

2. PROBLEM STATEMENT

In this section, we are going to describe about existing system and its disadvantages. The existing system mainly focuses on an external threat model. That is why the attacker within the wireless network can easily establish the selective jammingattack. There are two reasons for this problem, first one is the broadcast communication between nodes within the wireless network and second one is that the existing system uses the Spread Spectrum concept.

Conventional anti jamming technique use Spread Spectrum (SS) communication. The Spread Spectrum system take a user bit stream and perform an XOR with a pseudo noise sequence.Figure 1 is the spreading of the user data with the pseudo noise. The spread signal is then modulated with a radio carrier. Suppose for an example a user signal with a bandwidth of 1 MHz spreading with the PN code (10110111000 - known as 11-chip Barker code) would result in a signal with 11 MHz bandwidth. The radio carrier then shifts this signal to the carrier frequency (2.4 GHz in the ISM band). This signal is then transmitted.Figure 2 shows the simplified block diagrams of SS receiver. The SS receiver is more complicated than transmitter. The first step in the receiver involves demodulating the received signal. The receiver has to know the original PN code. This is the one main drawbacks of the existing system.

Spread Spectrum technique provides bit-level protection by spreading bits according to a secret pseudo noise (PN) code. That is known only to the communicating parties. This method can only protect the wireless networks under an external threat model. We know that the communication within the wireless network is done through the broadcast communication. So, this is vulnerable under an internal threat model. All intended receivers must know about the secrets used to protect transmissions. Another one drawback is compromise of a single receiver. So, the sender needs to reveal relevant cryptographic information to its receiver. A packet hiding technique is introduced for sending messages among nodes within the wireless network [4].

The following sections describes about packet hiding and wormhole concept.

3. PROPOSED SYSTEM

A solution to the selective jamming attack in the wireless network would be the encryption of packet that is going to send. Here encryption is applied to the attributes except destination. It means that we hide the packet from attacker. The encryption is applied only to the attributes except destination. That is why, during broadcasting there is no need for intermediate decryption. Each node checks the IP address of incoming packet. If it is sent for that particular node it will decrypt otherwise just forwarded to the next node.Alejandro Proano and LoukasLazos [4] proposed technique known as the Strong Hiding Commitment Scheme (SHCS) for packet hiding. This technique is based on symmetric cryptography [6][7]. First, the sender‘s’ has a packet ‘P’ for a particular receiver ‘r’. First step in SHCS is applying a permutation on packet P. That is, π_1(P). Then encrypt the corresponding permuted packet with a random key ‘k’. Here we can apply the Advanced Encryption Standard (AES) technique. Now the encrypted value became $c=E_k(\pi_1(P))$. This packet is broadcast to all nodes. Already told that, here encryption is applied only to the attributes except destination. Therefore an attacker within the wireless network can’t identify the source of incoming packet, because the packet is encrypted. Packet hiding methods make it difficult for attacker to identify its targeted node’s messages[8][9].

One question arises here is that, how the node can identify that a particular node is a jammer. The answer for this question is that a node which receives repeated acknowledgements for the same message or another situation is that the packet is held by a node in the network for a long time (not because of high network traffic) or if any node that violates the rules in a particular network region. Then the access point can identify that the particular node is a jammer.In this situation, the wormhole concept is newly incorporated. The access point then turns into a wormhole. This wormhole then prevents the jamming activity of particular jammer. By this method, all other nodes within that network can understand information about the jammer. Next time when they send a message, they can select another path for transmitting message or transmit through the same path, but must apply the packet hiding technique.

The packet can also be send through a shortest path between source and destination. Any algorithm for finding the shortest path between a source and destination can be used. In wireless network, it is possible to find the path by analyzing the range of nodes. Figure 3 shows a process flow, which describes the overall working of this concept when we implement it as practical.

Simulation of this proposed technique can be done by performing operations shown in the process flow. NODE CREATION module creates the nodes in wireless network. When we create a node we must specify the range of that particular node, because it is essential for the calculation of shortest path. Nodes can move from one position to another position. Suppose if one node is selected as a jammer, then the source send packet after applying SHCS technique and transmit through shortest path between source and destination.

The application of this concept arises when we require a secure communication such as emergency response operations, military, or police networks or safety-secret business operations. Just take an example, in emergency response operations like after a natural disaster, adhoc networks could be used for real-time safety feedback. In this situation, the usual network may be damaged. Emergency rescue groups might rely upon the adhoc networks for communication within that affected place.

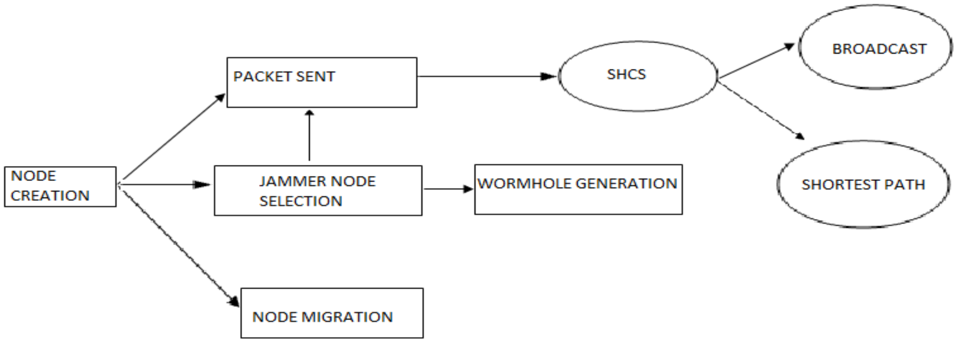

Figure 3. Process flow

4. IMPLEMENTATION

The proposed method is simulated by creating a virtual network using Java Thread API. Each node is created using as separate thread, it is possible to assign each node its position, auto IP assignment, routing table updating. Java.awt.graphics, javax. Swingcolour packages are used for creating the environments. A jammer node is created using thread and graphics packages for applying selective jamming. A node can berepositioned to any location. A wormhole is generated automatically to migrate from one place to another using graphics API. An alarm is generated by the wormhole as packet to every node in the region.

4.1 Network model

The network consists of a collection of nodes connected through wireless links. Nodes can be communicating either directly (if they are within communication range), or indirectly through multiple hops. Here both unicast and broadcast mode communications are possible. If there is no jammer, unencrypted communication can be performing. Otherwise encrypted communications might perform. For encrypted broadcast communications, packet will send after applying packet hiding method.

4.2 Communication model

The source sent message to its destination either directly or indirectly. When the source gets the information about jammer, it hides the packet and sends again through the same path. Implementation of packet hiding method is described in section 4.3. A wormhole also generates and it alerts all access points in the network about the presence of jammer. In section 4.4, we describe implementation details of wormhole.

4.3 SHCS implementation

The sender‘s’ has packet ‘P’ for a receiver ‘r’. The implementation of Strong Hiding Commitment Scheme technique has following steps:

- First apply a permutation on packet ‘P’. i.e., π_1 (P).
- Encrypt the permuted packet π_1 (P) with static key ‘k’ except destination part. We obtain the commitment value, c= E_k (π_1 (P)).
- The sender broadcast this commitment value along with static key ‘k’.
- At the receiver side, the reverse of above steps will take place.

Wormhole implementation

Wormholes can be used as a reactive defense mechanism. After receiving repeated acknowledgements, the source becomes the wormhole and sends the information regarding the jammer to all other nodes. This wormhole, then prevent the jamming activity of particular jammer. By this method, all other nodes within that network can understand the information about the jammer.

4.5 Shortest path implementation

Using the communication ranges between nodes, the shortest distance is calculated. A routing table is maintained to store the distance between nodes in a network. Updations are possible to the table whenever necessary.

5 PERFORMANE ANALYSIS

In [4], Alejandro Proano and LoukasLazos evaluate the impact of our packet-hiding technique on the network performance through simulations. The SCHS requires the application of permutation and one symmetric encryption at the sender side. The receiver side, the inverse operations have to be performed. They can implement AES at speed of tens of Gbps/sec. These processing speeds are higher than the transmission speeds of most current wireless technologies.

Cagalj [3] evaluate the wormhole-based anti-jamming techniqueusing simulations written in Mat lab. From that evaluation, we can understand the frequency of number of success increases. The wormhole can effectively alert the presence of the jammer to other nodes. From this, we can understand theselective jamming attack can be effectively prevented by using packet hiding method and wormhole based anti-jamming technique. After including wormhole-based anti-jamming and transmission through shortest path, the performance of the packet hiding technique improved. It improves the performance and reliability of the wireless networks.

6 CONCLUSION

In this paper, a technique is proposed for sending message in wireless network even if an attacker is present. It also described the technique wormholes, which will alert all other nodes about the presence of a jammer. Here the packet sends through the shortest path between sender and receiver. After including wormholes and shortest path concept the performance of packet hiding method improved. This technique is very effective in emergency response operations, military, police networks etc. It improves the performance and reliability of wireless networks. Static key used for encryption can be extended in future by adding random key concept. The packet hiding technique can also be performed using another techniques like Cryptographic Puzzle Hiding Scheme(CPHS) and Hiding Based on All-or-nothing transformation(AONTs).

REFERENCES

[1] A.D.Wood and J.A. Stankovic, “Denial of service in sensor networks,” Computer, vol. 35, no. 10, pp. 54-62, oct. 2002.

[2] J. McCune, E.Shi, A.Perrig, and M.K.Reiter, “Detection of Denial-of-message attacks on sensor networks broadcasts”, Proc. IEEE symp. Security and Privacy, May 2005.

[3] Mario Cagalj, SrdjanCapkun, Jean-PierroHubau “Wormhole-Based Anti jamming Techniques in sensor networks”, IEEE Transactions on mobile computing, vol. 6, no. 1, Jan 2007.

[4] AlejandroProano and LoukasLazos, “Packet-Hiding methods for preventing Selective Jamming attack”, IEEE Transactions on dependable and secure computing, vol. 9, no. 1,Feb-2012.

[5] I.Akyildiz,W.Su,Y.Sankarasubramaniam, and E.Cayirci, “A Survey on Sensor Networks,” IEEE Comm. Magazine, vol. 40, no, 8, 2002.

[6] K. Gaj and P. Chodowiec, “ FPGA and ASIC Implementations of AES”,Cryptographic Engineering, pp. 235-294 , Springer, 2009.

[7] O. Goldreich, “Foundations of Cryptography: Basic Applications”, Cambridge Univ. Press,2004.

[8] W.Xu,W.Trappe,Y.Zhang, and T.Wood, “The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks”, proc. MobiHoc ’05, pp.46-57, 2005.

[9] B. Schneier, “Applied Cryptography: Protocols, Algorithms, and Source Code in C”, 2007.

[10] W. Xu, T. Wood, W. Trappe, and Y. Zhang, “Channel Surfing and Spatial Retreats: Defenses against Wireless Denial of Service,”Proc. Third ACM Workshop Wireless Security, pp. 80-89, 2004.

Authors

DR. JAYASUDHA. J .Sis working as Professor and Head in the Department of Computer Science & Engineering, SreeChitraThirunal College of Engineering, Thiruvananthapuram. She has 18 years of teaching experience. She has organized many community development programmes, short term courses and conferences. She did her B. E. degree from Madurai Kamaraj University and M. E. degree from National Institute of Technology, Trichy and doctorate degree from University of Kerala. Her Ph.D. thesis title is “Web caching and Pre-fetching techniques for Web traffic/Latency reduction”. She is recognized as approved research guide in thePh.D. programme in Computer Science and guiding Ph.D. students in ManonmaniamSundaranar University and Noorul Islam University. Now she is also doing research in Computer Networks. She has published her research works in many national and international conferences and journals

DIVYA ANN LUKE currently doing her M.TECH degree in Computer Science & Engineering at SreeChitraThirunal College of Engineering, Thiruvananthapuram. She received her B.TECH degree in computer Science & Engineering from University of Kerala in 2012.Her research i nterests include the design and analysis of security and network protocols for wired and wireless networks.