Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 10, October 2014, pg.25 – 28

RESEARCH ARTICLE

PREVENTION OF SELECTIVE JAMMING ATTACKS USING PACKET HIDING METHODS IN WIRELESS NETWORKS

Rasamalla Naresh[1], K.Pranav Kumar[2]

[1]Pursuing M.Tech in SE & JNTU Hyderabad, India

[2]Department of CSE ARTI, Warangal, Telangana, India

[1] nareshrasamalla1225@gmail.com, [2] pranavkumar47@gmail.com

Abstract - The wireless networks always exposed to deliberate intrusion attacks referred to as jamming attacks. The wireless medium is more responsive to the Denial-of-Service (DoS) attacks. This is primarily focused on an exterior threat model. In wireless system the interactions between nodes get set through broadcast communication. therefore, whether an attacker is there inside the network can simply pry the message dispatched by whichever node. The major attack existing in the wireless system is the selective jamming attack. This kind of attack mostly naves a particular node termed as target node. Attacker at all times tries to prevent the message sent by the target node. This proceeds to the Denial-of-Service attack. We are presenting a novel technique to block the selective jamming attack in an interior threat model. Using packet hiding technique, we can transmit a message through the network however a jammer is there. This process is based on the technique named as Strong Hiding Commitment Scheme (SHCS).Whenever it detects any node that abuses the regulations in a meticulous network area. Afterward that node is considered as a jammer node. To conquer these attacks, we expand three proposals that avert the attacker from violating the packets. We are evolutions real time packet arrangement compounding cryptographic naives with imputed of physical layer also we evaluate computational and communique overhead in the security study.

Keywords— Denial-of-Service attack, AES, wireless networks elements, Selective jamming

I. INTRODUCTION

The wireless networks are more responsive to the Denial-of-Service (DoS) attacks [1]. Almost in each case, jamming causes a denial of service attack to any sender or receiver. The easiest way of jamming a wireless network communication is to repeatedly send ineffective data to the node where the server becomes congested. This attack builds the network resource engaged to its genuine users. This technique principally pointed on an exterior threat model. In broadcast communication when an attacker exists within the network can simply spy the message transmit by every node. In selective jamming attack methodology, the attacker constantly tries to prevent the message transmit by its objective node and it guides to the Denial-of-Service attack [1] [2].

In this docket, major focus is to block selective jamming attack in an interior threat representation. A wormhole[3] is used to produce an alarm to point out the incidence of jammer to every access point in the network. Existence of any jammer is discovered a technique called packet hiding [4] is used to send message throughout the network.

This process is based on the method called Strong Hiding Commitment Scheme(SHCS) [4]. Wormhole based anti-jamming design along is incorporated in the recently proposed scheme for preventing DoS attack.

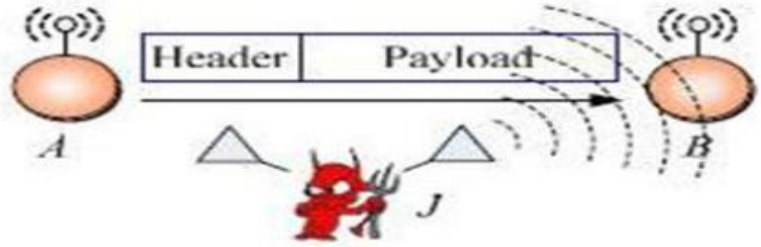

Fig1:Realization of a selective jamming attack

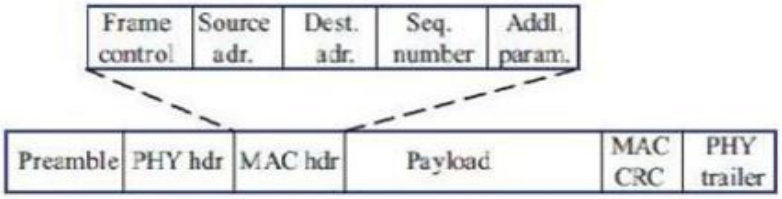

Fig. 1 A Generic frame format for a wireless network.

II. EXISTING SYSTEM.

The existing system mostly focused on an exterior threat replica. So that the attacker inside the wireless network can simply create a selective jamming attack. There are two motives for this difficulty, one is the broadcast communication among nodes surrounded by the wireless network and other one is that the presented system uses the Spread Spectrum conception. Spread Spectrum technique provides bit-level security by distributing bits according to a furtive pseudo noise (PN) code. That is identified only to the communicating parties.

This process can only defend the wireless networks in an external threat model. We recognize that the communiqué inside the wireless network is done all the way through the broadcast communication. So, this is susceptible under an interior threat model. All proposed receivers have to recognize about the secrets used to secure transmissions. An additional disadvantage is concession of a single receiver. Then the sender desires to expose applicable cryptographic data to its beneficiary. A packet hiding technique is commenced for transmitting messages amid nodes inside the wireless network [4].

III.PROPOSED SYSTEM

A clarification to the selective jamming attack in the wireless network would be the encryption of packet which is going to drive. Here encryption is only functional to the attributes excluding destinations. This denotes that we conceal the packet from attacker. Because of that, for the duration of broadcasting there is no demand for transitional decryption. Apiece node ensures the IP address of incoming packet. Whether it is transmit for that fastidious node it will decipher or else immediately forwarded to the subsequently node.

In this projected work we offer two new methodologies to transmit data among the server and many clients in the protected way. Earliest the information encryption technique is managed by the RSA Algorithm. Then the encrypted content is transmitting over the network .A Strong Hiding Commitment Scheme (SHCS) is implemented for pocket hiding technique. primarily, the sender‘s’ has a packet ‘P’ for a peculiar receiver ‘r’. initial step in SHCS is applying a permutation on packet P i.e. $\pi 1(P)$. After that encrypt the resultant permuted packet by a random key ‘k’. At this point we know how to relate the Advanced Encryption Standard (AES) technique. At this instant the encrypted value became $c=Ek(\pi 1(P))$. This packet is transmit to each and every node. previously pointed that, now encryption is practical only to the attributes except for destination. thus an attacker inside the wireless network can’t recognize the source of incoming packet,

since the packet is encrypted. Packet hiding methods create it complex for attacker to make out its targeted node's messages [8][9].

This part describes how rival categorizes the packet in real time earlier than the genuine packet is send to destination. At Physical layer, a packet k is programmed, interleaved & transformed before sending. At the receiver, the signal is demodulated, de-interleaved and deciphered to recuperate the unique packet.

The packet can in addition to be drive through a straight path among source and destination and any algorithm for verdicting the straight path among a source and destination can be utilized where as in wireless network, it is probable to get the path by considering the collection of nodes. Figure 3 shows a process flow, that explains the entire functioning of this conception when we apply it as practical. replication of this projected method can be done by performing operations shown in the process flow.

NODE CREATION module generates the nodes within wireless network. When we make a node we have to state the assortment of that specific node, since it is necessary for the computation of minimal path. Nodes can shift from one point to another point. If Suppose one node is chosen as a jammer, then the source transmit packet after validating SHCS technique and sent via minimal path among source & destination.

The application of this idea occurs when we need a protected communication such as crisis response operations, military, or police networks or safety-secret business maneuvers.

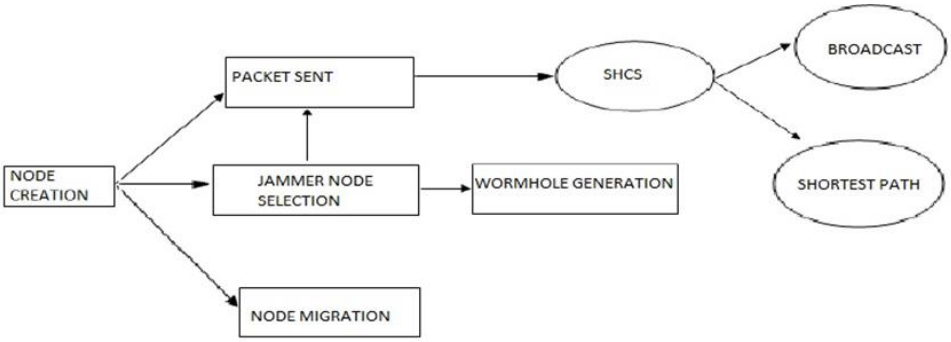

Fig. 2 Process Flow.

IV. IMPLEMENTATION

Initiate Server, Intermediate Server and 'n' number of nodes Node chooses a file 'F' to send file data to server. If node chooses the technique 'SHCS'(A Strong Hiding Commitment Scheme), the message block m is encrypted and encrypted message m| sent to receiver, where receiver decrypts and receives the message block m. If node chooses the technique 'Cryptographic Puzzle Hiding Scheme (CPHS)', the message block m is encrypted, a puzzle P and time duration tp is generated at the sender side and sent to receiver, where receive must solve the puzzle in the given duration tp and gets the decrypted message m.

If node chooses the technique 'AONT' (Hiding Based On All-Or-Nothing Transformations), the message block m is partitioned into n number of blocks. Then the blocks are encrypted and sent to receiver. The receiver the blocks are If node chooses the technique 'MD5' (Message Digest), the message block m is split into n number of blocks. Then the blocks are encrypted and sent as four round trips to receiver. In the receiver the blocks are decrypted and the sequence is checked and received.

A. Network model

A network comprises of similar or dissimilar collection of nodes connected through wired or wireless links where each node can communicate either directly (if they are within communication range) or indirectly through multiple hops in either unicast or broadcast or both modes of communication as possible unless there is no jammer installed unencrypted communication can be performed and data can be sent and received otherwise encrypted or decrypted communication might perform, in case of encrypted broadcast communication a packet will be sent after applying effective packet hiding method.

B. Communication model

A message is sent from source node to desired destination node in a direct or indirect fashion but when the source gets the information about jammer it simply hides the packet and sends again through the same path and the implementation of packet hiding method is further described in section 4.3. A wormhole also generates signal and alerts all access points which are registered for notifications in the network about the presence of a jammer.

C. 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 end the reverse of above steps will take place.

D. Wormhole implementation

Wormholes can be used effectively as reactive defense mechanism where a acknowledgement is repeatedly received by the source node it simply becomes the wormhole and sends the information regarding the jammer to all other nodes and only then the prevention of jamming activity by a identified jammer can be handled. By this method all other nodes within that network can understand the information about the presence of a jammer.

E. Shortest path implementation

Using the communication path which ranges between nodes and the shortest distance among tow or more nodes is calculated by creating the routing table that is maintained to store the distance between two or more nodes in a network where updations are possible to the table whenever necessary in a linear or non-linear hashing method.

V. CONCLUSION

Packet hiding method is used to block the selective jamming attacks. This will progress the recognition of a jammer rapidly with minimum difficulty. The presented system not averts the real time packet arrangement. The Swarm intelligence algorithm is capable enough to acclimatize changes in network topology & traffic. The grouping of cryptographic prime values with the physical layer characteristics for blocking real-time packet organization and counteracting with the knowledge of the attackers.

REFERENCES

[1] 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.

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

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

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

[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.

