International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 3 Issue 3, March - 2014

Hide and Seek: Mitigating the Jammers by Hiding Packets to Seek Secure Transmission

Neeta M S
Dept of Computer Science and Engineering
T.John Institute Of Technology
Bangalore, India

Srinivasa H P
Dept of Computer Science and Engineering
T.John Institute Of Technology
Bangalore, India

***Abstract*— Wireless networks are most emerging with its fascinating applications that make our day to day works most compact and easy. Security in such network is important, as these networks are prone to intentional interference attacks. Such attacks lead to denial of service attacks which is known as jamming. Jamming was previously addressed based on external threat model however for internal threat model attacks are made on messages of high interest such as route request reply by knowing the network secrets and protocol specifications. Such kind of jamming is known as selective jamming. In this paper we address the problem of selective jamming by making it random one. To mitigate this selective jamming attack real time classification is prevented by combining cryptographic methods with strong hide commitment scheme, cryptographic puzzle, all or nothing transformation and hash based hiding scheme along with PHY layer attributes that is addressed using TCP protocol.**

Index Terms—Jamming, Denial of Service, Authenticated node, Hash technique.

I. INTRODUCTION

As wireless networks are becoming more epidemic, ensuring the dependability of wireless network deployments will become an issue of critical importance. These wireless networks are prone to radio interference attacks that can be termed as jamming attacks. Due to the open nature of wireless networks and easy access to commodity devices that can be purchased and reprogrammed to interfere with communications, jamming can be launched with less efforts. Earlier jamming was considered under external threat model where jamming strategies include the continuous or random transmission of high power interference signals. This was overcome by considering the spread spectrum techniques .Later jamming was considered under internal threat model where adversary is intelligent to note the network details and protocol specifications. Thus adversary being intelligent concentrated on messages of high importance. In order to do this kind selective jamming the adversary must classify and jam. Thus adversary jammed with low efforts and made it difficult to counter.

In this paper we aim at mitigating the selective jamming and also prevent the packet classification by jammer. Security is enhanced by allowing only authenticated nodes to transmit message in the network. We address the problem of packet classification by encoding, interleaving channel and transmitting the packet using one among the four cryptographic hiding techniques such as strong hiding commitment scheme, hiding using cryptographic puzzle, all or nothing transformation and hash based hiding technique.

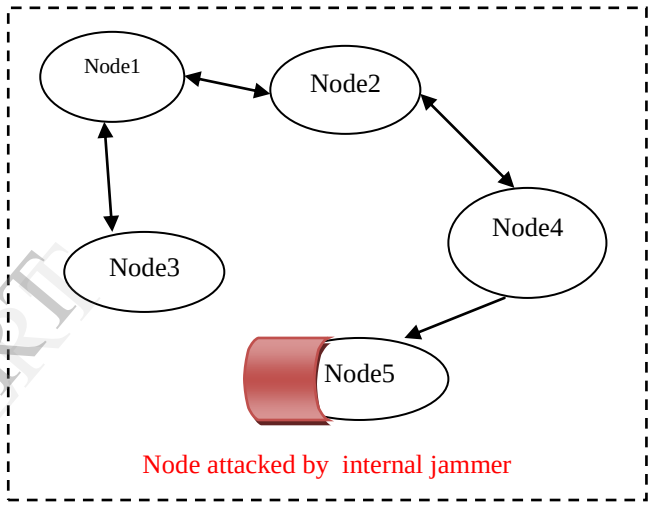

fig. 1.Typical jamming model in wireless network

II. RELATED WORK

In paper[1] the problems addressed are first, conducting radio interference attacks on wireless networks. Second examining the critical issue of diagnosing the presence of jamming attacks. To address the above problem **W. Xu, W. Trappe, Y. Zhang, and T.Wood** focussed on how radio jamming may be conducted and the tasks needed to detect these jamming attacks. In this paper four network attack models are being addressed they are constant jammer, deceptive jammer, random jammer and reactive jammer these various attack models will have different levels of effectiveness. The strategies implied to detect these attacks are first scheme employs signal strength measurements as a reactive consistency check for poor packet delivery ratios, while the second scheme employs location information to serve as the consistency check. Thus by this paper we understand different types jamming attacks and schemes to overcome these attacks that rely on external specifications of the threat .

In paper[2] **D. Thuente and M.Acharya** consider a particular class of Denial of Service (DoS) attacks called jamming is considered under the MAC layer. Here intelligence to the jammer is provided by using knowledge of the protocol

and exploiting crucial timings and control packets. In this paper various protocol aware jamming attacks that can be launched in an access point based 802.11b network are considered. By this paper we understand how the selective jamming is done by considering the intelligent adversary.

In paper [3] **P.Tague, M.Li, and R.Poovendran** addresses the problem of control channels that serve as a single point of failure which are targeted by a malicious adversary. The use of distinct, dedicated communication channels to transmit data and control traffic introduces a single point of failure for a denial of service attack, in that an adversary may be able to jam control channel traffic and prevent relevant data traffic. Hence, it is of interest to design control channel access schemes which are resilient to jamming. Here the problem mapped for providing resilient control channel access under jamming to that of secure communication channel establishment. In this work the use of random key distribution for resilience to control channel jamming is proposed so as to hide the location and frequency of control channel. In this paper security is provided to control channel by using random key distribution.

In paper[4] **Timothy X Brown Jesse E. James Amita Sethi** considers the problem of an attacker disrupting an encrypted victim wireless ad hoc network through jamming. Jamming and sensing are two related functions in physical-layer based denial of service attacks against an encrypted wireless ad hoc networks. Such attacks are made on the encrypted packets whose packet type and timing are known . This paper suggests simple methods for making victim networks less vulnerable to these kinds of attacks.

A. Disadvantages of Existing System

- Bit-level Protection under external threat model .
- Packets are prone to attacks , when attacker uses internal details of threat model
- Broadcast communications are particularly vulnerable under internal threat models as all receivers are aware of secrets used to protect transmission.
- Before transmission packets are classified and jammed.

III. PROBLEM STATEMENT AND ASSUMPTIONS

A. Problem Statement

Communication exists between node A and node B in a wireless network. There exists a jammer node J in the communication range of A and B. When A transmits packets p to B , node J classifies packets p add error bits to few bytes of the packets .Thus making packets unreachable to receiver by interfering in its recovery at B. Here we address the problem of preventing jammer from disabling packet transmission and classification of packet to jam it.

B. Network Model

Network consists of a collection of nodes which are authenticated to transmit the message in wireless network. Packets are transmitted both encrypted or unencrypted manner. Nodes may communicate directly if they are within communication range, or indirectly via multiple hops.

C. Communication Model

The packets are transmitted via wireless networks, these transmitted packets have the generic format depicted in above figure. The preamble is used for synchronizing the sampling process at the receiver. The PHY layer header contains information regarding the length of the frame, and the transmission rate. The MAC header determines the MAC protocol version, the source and destination addresses sequence numbers plus some additional fields. The MAC header is followed by the frame body that typically contains an ARP packet or an IP datagram. Finally, the MAC frame is protected by a cyclic redundancy check (CRC) code. At the PHY layer, a trailer may be appended for synchronizing the sender and receiver.

D. Adversary model

We assume adversary under the control of communication medium can operate in both full duplex and half duplex mode so that it can jam any part of the network simultaneously during transmission and reception. The adversary is equipped with directional antennas that enable to receive the signal from one node and jamming the same in the another node.The adversary is assumed to be computationally and storage bounded, although he can be far superior to normal nodes. In particular, he can be equipped with special purpose hardware for performing cryptanalysis or any other required computation. Thus the adversary is capable of physically compromising network devices and recovering stored information including cryptographic keys, PN codes etc.

IV. PROPOSED SYSTEM

Here we address the problem of jamming under the internal threat model. We consider adversary aware of network secrets and implementation details of network protocols at any layer of protocol stack that can launch low-effort jamming attacks which are difficult to detect and counter. Adversary utilizes the internal knowledge for launching attacks on messages of high importance. For example, a jammer can target route-request/route-reply messages at routing layer to prevent route discovery,. These selective jamming attacks on protocols like TCP and routing protocols significantly impact performance with low effort. Here we transform a selective jammer to a random one by preventing real-time packet classification and provide secure transmission by hiding the data between the authenticated nodes of the network during transmission using hiding techniques combining with cryptographic methods.

It has the following advantages:

- Security is provided by considering the cryptographic mechanisms with physical layer attributes. Thus strong security properties are achieved.
- The selective jamming attacks on protocols TCP and routing protocols significantly impact performance with low effort and hence selective jamming is transformed to random one.

- Strong security is gained by providing authentication to nodes .

V. Real Time Packet Classification

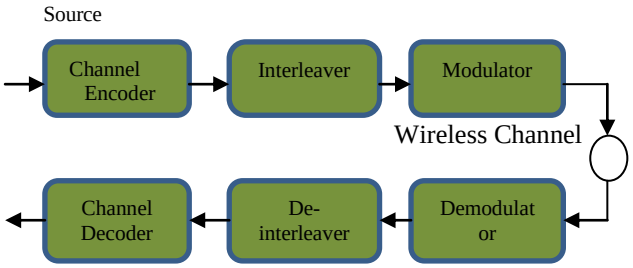

fig.2.Generic Communication System

. To prevent the packet classification the packet is sent as mentioned in the above model. Channel encoding block expands the original bit sequence p, adding necessary redundancy for protecting p against channel errors. At the next block, interleaving is applied to packet p from burst errors. we consider a block interleaver that is defined by a matrix $A_{d*\beta}$. The de-interleaver is simply the transpose of A. Finally, the digital modulator maps the received bit stream to symbols of length q, and modulates them into suitable waveforms for transmission over the wireless channel. Typical modulation techniques include OFDM, BPSK, 16(64)-QAM, and CCK. In order to recover any packet bit p, the receiver must collect d.β bits for de-interleaving. The d.β de-interleaved bits are then passed through the decoder. Thus finally packet is received.

V. Packet Hiding schemes and Outcomes

A. All Or Nothing Transmission

The packets are pre-processed by an AONT before transmission but remain unencrypted. The jammer cannot perform packet classification until all pseudo-messages corresponding to the original packet have been received and the inverse transformation has been applied. Packet p is partitioned to a set of x input blocks p= $\{p_1, p_2, p_3 \ldots p_x\}$, which serve as an input to an The set of pseudo-messages $p' = \{p'_1, p'_2, p'_3, \ldots .p'_x\}$ is transmitted over the wireless medium. At the receiving end inverse transformation of packet p pseudo message is received, in order to recover the original message.

B. Hiding Based On Cryptographic Puzzle

A sender S has a packet p for transmission. The sender selects a random key k , of a desired length. S generates a puzzle (key, time), where puzzle() denotes the puzzle generator function, and tp denotes the time required for the solution of the puzzle. Parameter is measured in units of time, and it is directly dependent on the assumed computational capability of the adversary, denoted by N and measured in computational operations per second. After generating the puzzle P, the sender broadcasts (C, P). At the receiver side, any receiver R solves the received puzzle within the specified time to recover key and then computes to get the original message.

C. A Strong Hiding Commitment Scheme

A strong hiding commitment scheme (SHCS) is based on symmetric cryptography. Assume that the sender has a packet p for Receiver. First, S constructs commit of message m (C,d)=commit(m) where,

$$C=E_k(\pi_1(m)),\ d=k$$

the commitment function is an off-the-shelf symmetric encryption algorithm π_1 is a publicly known permutation, and k $\in\{0,1\}^s$ is a randomly selected key of some desired key length s (the length of k is a security parameter). Sender sends (C||d) to receiver which is computed as

$$m=\pi^{-1}_1(D_k(C))$$

To satisfy the strong hiding property, the packet carrying d is formatted so that all bits of d are modulated in the last few PHY layer symbols of the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d.

D. Hash Based Hiding Technique

A cryptographic hash function is a hash function that takes an arbitrary block of data and returns a fixed-size bit string, Message to be sent is encrypted by key which is hashed using MD5 algorithm. The hashed key is mailed to recipient . At the receiver hashed key is entered to recover the original message. This hashed key is passed through the Internet as a data packet. TCP header is a most common part of the data packet. There are six reserved bits which remains always unused in TCP header. Here using these unused bits of header security of the key is enhanced to gain secure transmission.

E.Outcome

The registered node are authenticated to transmit the message between the node A and node B in an wireless network, channel is encoded and interleaved to prevent real time packet classification.

Packet is mapped by hiding schemes to prevent the jammer J from blocking the transmission.

Message undergoes a transformation in all or nothing scheme where original message is transformed to a pseudo message before it subjected to symmetric encryption. At the receiving end inverse transformation of pseudo message is carried to recover the original message using key.

During cryptographic puzzle based hiding scheme , the puzzle is generated using which the message is encoded and sent to the receiver along with specified time stamp. Original message is decrypted at the receiving end by computing the given puzzle within mentioned time stamp.

Packet is hided using symmetric encryption. To satisfy the strong hiding property, the packet carrying d is formatted so that all bits of are modulated in the last few PHY layer symbols of the packet. To recover d, any receiver must receive and decode the last symbols of the transmitted packet, thus preventing early disclosure of d.

Hashing technique is included to enhance security of packets by mailing the hashed value of key to authenticated receiver. By using this key original message is recovered.

VIII. CONCLUSION

In proposed work we addressed jamming in the wireless network which are due intentional interference attacks in the network. Here jamming is considered under internal threat model where the jammer is aware of network secrets and also protocol specifications. Using this knowledge packet was classified and jammed that resulted in selective jamming. Security is enhanced by allowing only authenticated nodes to transmit message in the network. To address the problem of selective jamming, real time classification is to be prevented by combining cryptographic methods with strong hide commitment scheme, cryptographic puzzle, all or nothing transformation and hash based hiding scheme along with PHY layer attributes that is addressed using TCP protocol.

REFERENCES

[1] W. Xu, W. Trappe, Y. Zhang, and T.Wood. The feasibility of launching and detecting jamming attacks in wireless networks. *In Proceedingsof MobiHoc, pages 46–57, 2005.*

[2] D. Thuente and M. Acharya. Intelligent jamming in wireless networks with applications to 802.11 b and other networks. *In Proceedings of the IEEE Military Communications Conference MILCOM, 2006.*

[3] P. Tague, M. Li, and R. Poovendran. Probabilistic mitigation of controlchannel jamming via random key distribution. *In Proceedings of PIMRC, 2007.*

[4] 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.*

[5] Alejandro Proano and Loukas Lazos. Packet-Hiding Methods for Preventing Selective Jamming Attacks *In Proceedings of IEEE Transactions On Dependable And Secure Computing ,Vol. 9, No. 1, Jan-Feb 2012.*

[6] Y. W. Law, M. Palaniswami, L. V. Hoesel, J. Doumen, P. Hartel, andP. Havinga. Energy-efficient link-layer jamming attacks against WSN MAC protocols. *In Proceedings of ACMTransactions on Sensors Networks, 5(1):1–38, 2009.*

[7] W. Xu, T.Wood,W. Trappe, and Y. Zhang. Channel surfing and spatial retreats: defenses against wireless denial of service. *In Proceedings of the 3rd ACM workshop on Wireless security, pages 80–89, 2004.*

[8] Abhimanyu.V ,L.M.Nithya Enhanced Techniques for Preventing Selective Jamming *In Proceedings of NCNICS 2013 Issue ISSN 2278-733X*

[9] Mary Cindy Ah Kioon, ZhaoShun Wang and Shubra Deb Das Attacks Security Analysis of MD5 algorithm in Password Storage *In Proceedings of the 2nd International Symposium on Computer, Communication, Control and Automation (ISCCCA-13)*

[10] en.wikipedia.org/wiki/Cryptographic_**hash**_function