Detection of attacks based on timestamp discrepancy

Ms. Pratibha S. Gaikwad, Prof. S. P. Pingat

Abstract— **In this era of digital physical frameworks, wireless networking applications has been drawing expansive interest of studies. Due to the shared nature and the open access to the wireless medium, jamming attacks have become common problem during the last few years. Main objective of writing this paper is to address some basic attacks like jamming and replay attack in wireless application and how these attacks can be detected and prevented in wireless applications. An attacker can perform replay attack; this can be done at anytime and any-where in the network by simply interception and retransmission of the valid messages. Finding the exact location of an attacking device is of great importance for restoring normal network operations. Our goal in this paper is to detect and prevent these attacks using concept of timestamp and filtering technique. After detecting the actual malicious node we want to block that node to restore system to normal network operations.**

Index Terms—**Jamming attack, packet replay attack, timestamp.**

I. INTRODUCTION

Wireless technologies have become increasingly popular in our day to day business and personal lives. Wireless communications gives both adaptability and expense savings in deployment and maintenance as compare to wire lined deployments. As these networks achieve popularity, providing security and trustworthiness are the basic issues. However, their shared nature and open access makes them highly susceptible to different types of attacks. Due to these reasons, different types of attacks detection are a primary concern from researcher point of view. Paper presents a particularly attacks like jamming and replay attack. A jammer can be characterized as an element who is attempting to interfere with the transmission and gathering of wireless communications. A jammer can achieve this objective by either keeping a genuine traffic source from conveying a bundle, or by keeping the gathering of honest to goodness packets. There are many different attack strategies that a jammer can perform in order to interfere with wireless communications. Some possible strategies are given below.

Constant Jammer: A constant jammer continuously emits a radio signal (noise) that represents random bits; this radio signal generated does not follow any protocol. The device dose not even waits for the medium to become idle for transmission.

Deceptive jammer: Deceptive jammers inject semi-valid packets with no gap between packets which means packet header is useful but payload is useless. So device will remain in the receive state and never switch to the send state due to constant flow of incoming packets.

Random Jammer: Random jammer alternates between sleeping and jamming. It can act as constant or deceptive whenever jamming occurs.

Reactive jammer: The above three models are active jammers but this is not. It stays quiet until there is activity on the channel. This jammer concentrates on the reception of a message.

After jammer jam message, jammer holds message for some time and then it generate replay of same message to form redundant data at receiver side. A simple and effective strategy for wireless DoS is to replay locally heard data packets. These packets are then passed by other forwarding nodes which results in increased levels of congestion at reception side. Simple replay attack can be, where an adversary who captures the data and simply retransmits it.
Some possible replay attack strategies are:

The attacker does not manipulate any packet contents and the other one attacker edits the packet header. Therefore it is necessary to prevent these attacks which are vulnerable to wireless network. Many ideas have been proposed to prevent these attacks. Main objective of paper detect and prevent jamming and replay attack.

II. RELATED WORK

Xu et al. [3], studied feasibility of launching and detecting different types of jamming attacks. In this paper they conclude that using carrier sensing time, packet sent ratio and packet delivery ratio individually, one is not able to classify the presence of a jamming attack. So paper improved detection technique by introducing concept of consistency check. They have proposed two enhanced detection algorithm: one is taking signal strength as a consistency check and other considering location information as consistency check. Consistency checking scheme improves detection performance. Frequency of the location advertisement is critical to which directly affects performance.

Ali et al. [4], present scheme for detection of jamming attacks in wireless adhoc networks. They proposed new method error distribution to detect jamming attack and use the scheme called correlation to measure association between

Manuscript received June, 2015.

***Pratibha S. Gaikwad**, Department of Computer Engineering, Savitribai Phule Pune University, Smt. Kashibai Navale College of Engineering, Pune, India, 7387300799.*

***Prof. S. P. Pingat**, Department of Computer Engineering, Savitribai Phule Pune University, Smt. Kashibai Navale College of Engineering, Pune, India.*

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

two variables. Presented a new model based on the measure of correlation among error and correct reception time to identify presence of jamming attack in adhoc network. Main goal is to detect specific type of jamming attack. With the proposed method, able detect the presence of jamming attack with high degree of confidence. An advantage of proposed scheme is its simplicity and efficiency. If correlation relation is not linear then results are inaccurate.

In paper [5], they proposed a method to detect jamming attack in CSMA/CA network on basis of calculation of probability of collision in network. Paper presents robust nonparametric detection technique which is based on M-truncated sequential Kolmogorov-Smirnov statistics. Observe the unbeaten transmissions and the collisions of the terminals in the network, and conclude how "explainable" the collisions are given for such observations. This presented method provides very low detection latency and high detection accuracy. This scheme is robust, as it is capable to detect any deviation from normal operation without modifying existing protocol. They applied this test to detect intelligent jamming attack.

Li et al. [6], studied intelligent jamming attacks in wireless sensor network which are easy to launch and hard to detect. Adversary controls probability of jamming and transmission range to cause maximum harm to the network. Jammer is detected at monitoring node by applying optimal detection test based on percentage of incurred collision.

In paper [7], presents scheme broadcast dynamic jamming mitigation using the combination of spread spectrum and binary key tree. Proposed method provides high performance.

Liu et al. [8], studied different anti-jamming technique such as frequency hopping and direct sequence spread spectrum. Paper presents novel, efficient and robust method called USD-FH (Uncoordinated seed disclosure frequency hopping). Scheme provide secret key in the existence of adversaries. Uncoordinated seed disclosure frequency hopping make use of a one-time pseudo random hopping pattern to broadcast each DH key establishment message and then reveal the seed of the pseudo random hopping pattern in an uncoordinated form before the actual message transmission. Proposed scheme advantages are robust and most efficient than previous approaches.

In paper [10], they considers a variant of the data packet replay attack and these packets increases levels of congestion and interference enhance in large portions of the network. Adversary can either simply replay packet as it is or can modify packet header to make illusion of new packet. Presents detection and prevention technique COPS (for Copycat Online Prevention System). This technique uses combination of digital signature and bloom filters to deal with the attack. Proposed scheme consider only a percentage of packets is signed and load of verification is distributed along the nodes. Processing overhead is reduced by proposing attack mitigation using a combination of digital signatures and bloom filters. Advantages of this method, low resource consumption and processing overhead is reduced.

Table 1: Evaluation of related work

Paper name	Proposed	Advantage
The Feasibility of Launching and Detecting Jamming Attacks in Wireless Networks	Two detection algorithms: signal strength as a consistency check and location information as a consistency check.	Consistency checking scheme improves detection performance.
Detection of Jamming Attacks in Wireless Ad Hoc Networks using Error Distribution	Proposed a new method measurement of error distribution using correlation coefficient	Achieved simplicity, efficiency high and degree of confidence.
USD-FH: Jamming-resistant Wireless Communication using Frequency Hopping with Uncoordinated Seed Disclosure	Proposed USDFH: Uncoordinated Seed Disclosure in Frequency Hopping to establish a shared secret in presence of jammers.	More efficient and robust. Message is transmitted entirely, while all pervious solution has to split message into multiple pieces.
Optimal Jamming Attacks and Network Defense Policies in Wireless Sensor Networks	Proposed optimal detection test based on the percentage of incurred collisions.	During normal network operation and in absence of a jammer, it gives a large enough training period (percentage of collisions).
USD-FH: Jamming-resistant Wireless Communication using Frequency Hopping with Uncoordinated Seed Disclosure	Proposed USDFH: Uncoordinated Seed Disclosure in Frequency Hopping to establish a shared secret in presence of jammers.	More efficient and robust. Message is transmitted entirely, while all pervious solution has to split message into multiple pieces.
Coping with Packet Replay Attacks in Wireless Networks	Proposed COPS: Copycat Online Prevention System.	Processing overhead is reduced.

III. PROPOSED SYSTEM

In this paper, we provided an in-depth study on the impact of jamming and replay packet attacks in the wireless applications. It is very easy to launch jamming and replay attack but it is hard to detect. We design the system to achieve efficient and robust jamming and replay packet attack detection with prevention. Due to the shared nature and the open access to the wireless medium, jamming attacks have become common problem. As jammer jam the message and then attacker holds message for some time and then it generate replay of same message to form redundant data at

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

receiver side. The paper proposed concept of timestamp to detect jamming attack. Prevention is done by filtering the replay packet which is responsible for network jamming.

It also helps in detection and prevention attack like replay attack and blocking IP address of actual attacker in the network. Receiver node is responsible for detecting jamming and replay attack and prevention of actual attacker.

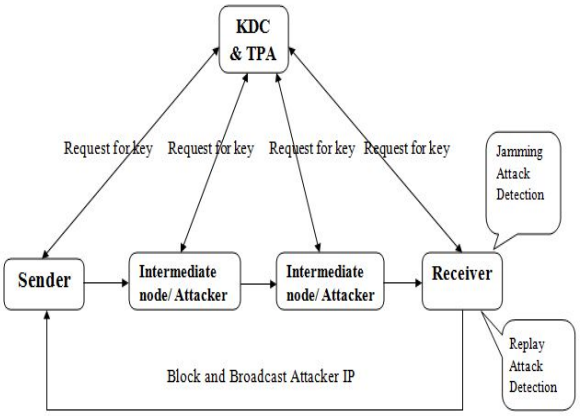


Fig.1. System architecture

IV. Experimental Setup

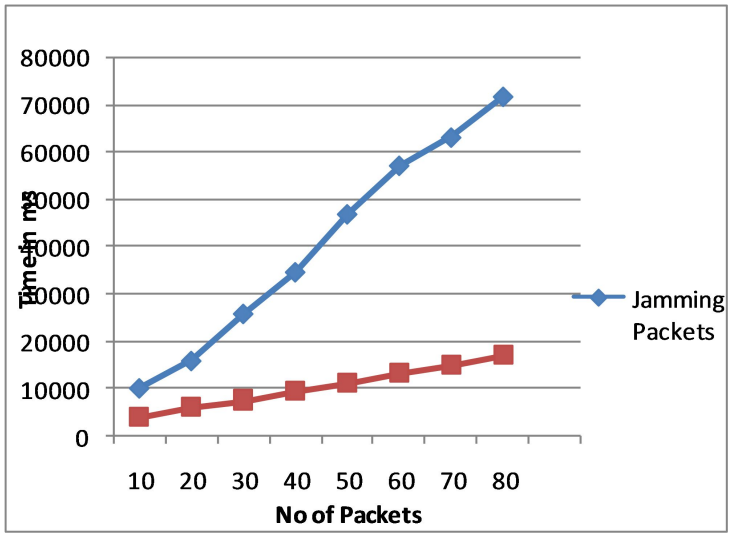
The system is built using Java framework (version JDK 8) on Windows platform. The NetBeans (version 8) is used as a development tool. Any standard machine is capable of running the application. The additional non functional requirement is the network should be connected while transmitting the packets.

V. Result and Discussion

The following table shows the number of packets needed to be transmitted under different circumstances. Below are the circumstances like, normal communication and with jamming attack.

Table 2: Result table

No. of packet to send	Normal packet sending time	Jamming packet sending time
10	4000	10000
20	5964	15790
30	7512	25758
40	9490	34573
50	11146	46837
60	13174	57110
70	14957	63080
80	16943	71708



The graph no of packets vs time shows that the time required for the transmission of no of packet for normal transmission and with jamming transmission of packets. With jamming attack transmission packet requires more time for the transmission as the attacker may hold the packets during packet forwarding through intermediate node.

VI. Conclusion

Proposed system gives idea about detection and prevention of jamming and replay packet attack. Detecting any type of attack is the first step in defeating it. In this paper we developed a novel, efficient and robust scheme to detect jamming and replay attack. Detection of jamming attack and packet replay attack is done by scheme called timestamp and packet filtering. We found actual adversary and prevents such type of adversary and broadcast IP address of actual attacker in network to restore system to normal network operation.

Acknowledgment

I am very thankful to the Savitribai Phule Pune University, Pune. I am highly grateful to my department and college, Department of computer engineering and Smt. Kashibai Navale College of Engineering to providing all the facilities.

I am thankful to my esteemed guide Prof. S. P. Pingat for expert and precise guidance.

References

[1] Pratibha S. Gaikwad, Prof. S. P. Pingat, "Detecting Jamming and Replay Packet Attacks in Time-Critical Wireless Applications" ,IJSR Jan 2015

[2] Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless applications Zhuo Lu, Student Member, IEEE, Wenye Wang, Senior Member, IEEE,and Cliff Wang, Senior Member, IEEE ,August 2014.

[3] Xu, W. Trappe, Y. Zhang, and T. Wood, "The feasibility of launching and detecting jamming attacks in wireless networks", in Proc. ACM MobiHoc, Urbana-Champaign, IL, USA, 2005, pp. 46-57.

[4] A. Hamieh and J. Ben-Othman, "Detection of jamming attacks in wireless ad hoc networks using error distribution," in *Proc. IEEE ICC*, Dresden, Germany, Jun. 2009.

[5] A. L. Toledo and X. Wang, "Robust detection of MAC layer denial-of-service attacks in CSMA/CA wireless networks," *IEEE Trans. Inf. Forensics Security*, vol. 3, no. 3, pp. 347–358, Sep. 2008

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET

[6] M. Li, I. Koutsopoulos, and R. Poovendran, 'Optimal jamming attacks and network defense policies in wireless sensor networks,' in Proc. IEEE INFOCOM, May 2007, pp. 1307-1315.
[7] Jerry T. Chiang, Yih-Chun Hu "Dynamic Jamming Mitigation for Wireless Broadcast Networks".
[8] An Liu, Peng Ning, Huaiyu Dai, Yao Liu "USD-FH: Jamming-resistantWireless Communication using Frequency Hopping with Uncoordinated Seed Disclosure", IEEE 2010.
[9] Zi Feng, Jianxia Ning, Ioannis Broustis "Coping with Packet Replay Attacks in Wireless Networks", IEEE 2011.

ISSN: 2278 – 1323 All Rights Reserved © 2015 IJARCET