ISSN 2395-1621

Survey Paper on Carousel attack and Stretch attack on WSN

[#1]Atul Sontakke, [#2]Rahul Jaybhaye, [#3]Vivek bagade, [#4]Sanket Chavan

[1]atsontakke@gmail.com,
[2]rahuljaybhayerj7@gmail.com
[3]vivekbagade7@gmail.com
[4]csanket48@gmail.com

[#1234]Department of Computer Engineering,

JSPM's,
Imperial College of Engineering and Research,
Wagholi, Pune.

ABSTRACT

In this paper we Survey on wireless networking using the different network attack technique. Considering the role of wireless adversary, which targets the packets of high importance by emitting radio frequency signals and do not follow underlying network architecture. Typically, jamming attacks have been considered under external threat model, in which jammer is not part of network. In this paper we proposed the new attack on WSN, carousel attack and stretch attack during the packet forwarding source to destination.

Keywords: **Jamming attack, Security, Routing, Ad hoc networks, Carousel attack, Stretch attack.**

ARTICLE INFO

Article History

Received: 1st December 2016

Received in revised form :

2nd December 2016

Accepted: 5th December 2016

Published online :

6th December 2016

I. INTRODUCTION

Wireless networks have paved the way for mobile nodes to communicate with each other. The two basic system models are fixed backbone wireless system and wireless Mobile Ad hoc Network (MANET).[2][3] A MANET is a collection of nodes that do not rely on a predefined infrastructure to keep the network connected. Therefore the functioning of ad hoc networks is dependent on the co-operation of each and every node. The nodes help each other in conveying information about the topology of the network and share the responsibility of managing the network. The rapid proliferation of wireless ad-hoc networks and mobile computing applications has changed the landscape of network security. Wireless networks are networks which provide users with connectivity regardless of their actual physical location. WSN's (Wireless sensor Networks) are a new type of networked systems, characterized by severely constrained computational and energy resources, and an ad hoc operational environment. [6]

Jamming Attack: - It is a type of DOS attack. There are many different attack strategies that a jammer can perform in order to interfere with other wireless communications. Some possible strategies are exposed below:

Constant Jammer: A constant jammer continuously emits a radio signal that represents random bits; the signal generator does not follow any MAC protocol.

Deceptive Jammer: Different from the continuous jammers, deceptive jammers do not transmit random bits instead they transmit semi-valid packets. This means that the packet header is valid but the payload is useless.

Random Jammer: Alternates between sleeping and jamming the channel. In the first mode the jammer jams for a random period of time (it can behave either like a constant jammer or a deceptive jammer), and in the second mode (the sleeping mode) the jammer turns its transmitters off for another random period of time. The energy efficiency is determined as the ratio of the length of the jamming period over the length of the sleeping period.

Reactive Jammer: A reactive jammer tries not to waste resources by only jamming when it senses that somebody is transmitting. Its target is not the sender but the receiver, trying to input as much noise as possible in the packet to modify as many bits as possible given that only a minimum amount of power is required to modify enough bits so that when a checksum is performed over that packet at the receiver it will be classified as not valid and therefore discarded.

II. LITERATURE SURVEY

Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo, "Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach", in this paper studied a CPS scenario where a malicious agent carries out jamming attacks on the communication channel between a sensor and a remote estimator. he first considered a situation where the sensor and the attacker fix their strategies apriori. For the case where the sensor and the attacker have on-line information about the previous transmission outcomes and the occurrence of attacks. [1]

Zhuo Lu,Student, "Modeling, Evaluation and Detection of Jamming Attack in Time-Critical Wireless Applications", in this paper, he provided an in-depth study on the impact of jamming attacks against time-critical smart grid applications by theoretical modelling and system experiments. He introduced a metric, message invalidation ratio, to quantify the impact of jamming attacks. He showed via both analytical analysis and real-time experiments that there exist phase transition phenomena in time-critical applications under a variety of jamming attacks. Based on our analysis and experiments, He designed the JADE system to achieve efficient and robust jamming detection for power networks. [2]

Nani Yalu, RajatSubhra Goswami, Subhasish Banerjee, "An Efficient Packet Hiding Method for Preventing Jamming Attacks in Wireless Networks", this paper have reviewed all packet hiding methods and addressed their merits and demerits. We have also compared different packet hiding methods and thus come up with the conclusion that all three packet hiding methods are highly secured but have their own shortfalls.[3]

Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems,", in this paper, he characterize the reachable set of the system state and estimation error under the attack, which provides a quantitative measure of the resilience of the system. To this end, we will provide an ellipsoidal algorithm to compute the outer approximation of the reachable set. He also prove a necessary condition under which the reachable set is unbounded, indicating that the attacker can successfully destabilize the system. [4]

Saurabh Amin, Alvaro A. C´ardenas, and S. Shankar Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks" he considers the problem of security constrained optimal control for discrete-time, linear dynamical systems in which control and measurement packets are transmitted over a communication network. The packets may be jammed or compromised by a malicious adversary. For a class of denial-of-service (DoS) attack models, the goal is to find an (optimal) causal feedback controller that minimizes a given objective function subject to safety and power constraints. He present a sem definite programming based solution for solving this problem. [5]

III. NETWORK DESIGN OBJECTIVES

Small node size: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers, reducing node size can facilitate node deployment. It will also reduce the power consumption and cost of sensor nodes.

Low node cost: Since sensor nodes are usually deployed in a harsh or hostile environment in large numbers and cannot be reused, reducing cost of sensor nodes is important and will result into the cost reduction of whole network.

Low power consumption: Since sensor nodes are powered by battery and it is often very difficult or even impossible to charge or recharge their batteries, it is crucial to reduce the power consumption of sensor nodes so that the lifetime of the sensor nodes, as well as the whole network is prolonged.

Scalability: Since the number sensor nodes in sensor networks are in the order of tens, hundreds, or thousands, network protocols designed for sensor networks should be scalable to different network sizes.

Reliability: Network protocols designed for sensor networks must provide error control and correction mechanisms to ensure reliable data delivery over noisy, error-prone, and time-varying wireless channels.

Self-configurability: In sensor networks, once deployed, sensor nodes should be able to autonomously organize themselves into a communication network and reconfigure their connectivity in the event of topology changes and node failures.

Adaptability: In sensor networks, a node may fail, join, or move, which would result in changes in node density and network topology. Thus, network protocols designed for sensor networks should be adaptive to such density and topology changes.

Channel utilization: Since sensor networks have limited bandwidth resources, communication protocols designed for sensor networks should efficiently make use of the bandwidth to improve channel utilization. Fault tolerance: Sensor nodes are prone to failures due to harsh deployment environments and unattended operations. Thus, sensor nodes should be fault tolerant and have the abilities of selftesting, self-calibrating, self-repairing, and self-recovering.

Security: A sensor network should introduce effective security mechanisms to prevent the data information in the network or a sensor node from unauthorized access or malicious attacks.

IV. METHODOLOGY

Carousel Attack Module :

:

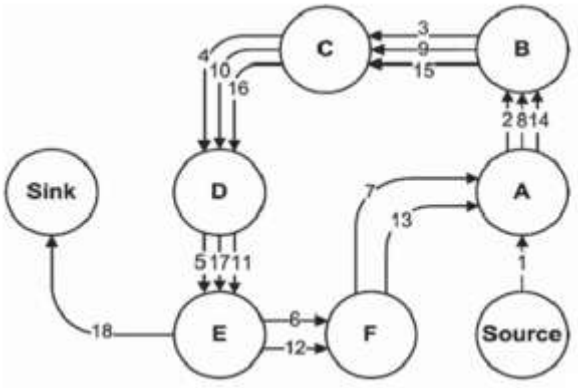

Fig 1. Carousel attack flow

In first attack, an adversary composes packets with purposely introduced routing loops. This is called as carousel attack, since it sends packets in circles. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route.

Stretch Attack Module:

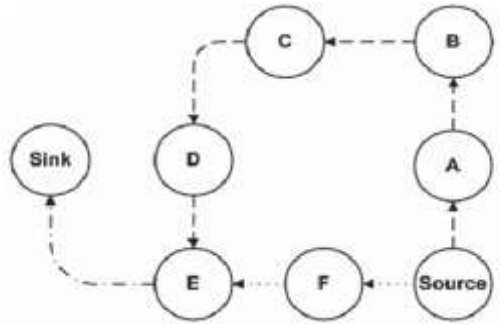

Fig 1. Stretch attack flow

In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. This is called as stretch attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. A single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node.

V. PROPOSED ARCHITECTURE

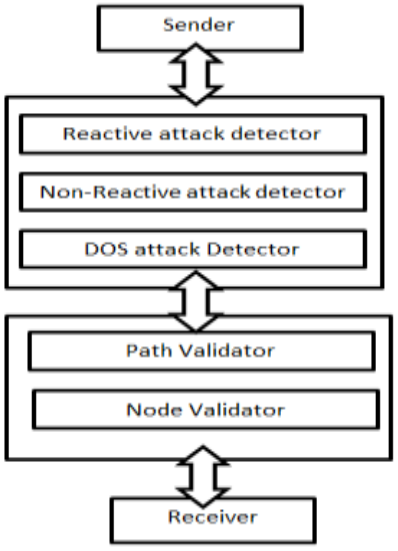

Fig 3. Proposed architecture

Reactive jammer: This type of jammer is quiet until the medium is idle and when it senses transmission on the medium it starts injecting false data which avoids the legitimate user to send data. Among all the above four jammers the reactive jammer is very difficult to detect.

Non-Reactive jammer: This type of jammer is quiet when your system will slow down. above jammers the non-reactive jammer is very simple to detect.

V. CONCLUSION

In this paper, we review the attacks in wireless networks. We also studied system models to introduce carousel attack and stretch attack during the packet forwarding source to destination. And attack detection model is also presented. Then we discussed real-time packet classification to classify the packet before reaching at destination.

REFERENCES

[1] Yuzhe Li, Ling Shi, Peng Cheng, Jiming Chen, and Daniel E. Quevedo, "Jamming Attacks on Remote State Estimation in Cyber-Physical Systems: A Game-Theoretic Approach", IEEE TRANSACTIONS ON AUTOMATIC CONTROL, VOL. 60, NO. 10, OCTOBER,2015.

[2] Zhuo Lu,Student Member, IEEE,Wenye Wang,Senior Member, IEEE, and Cliff Wang,Senior Member, IEEE "Modeling, Evaluation and Detection of Jamming Attacks in Time-Critical Wireless Applications" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 13, NO. 8, AUGUST 2014.

[3] Nani Yalu, RajatSubhra Goswami, Subhasish Banerjee, "An Efficient Packet Hiding Method for Preventing Jamming Attacks in Wireless Networks" IEEE WiSPNET 2016.

[4] Y. Mo and B. Sinopoli, "Integrity attacks on cyber-physical systems," in Proc. 1st Int. Conf. High Confidence Networked Syst., 2012, pp. 47–54.

[5] Saurabh Amin, Alvaro A. C´ardenas, and S. Shankar Sastry, "Safe and Secure Networked Control Systems under Denial-of-Service Attacks" R. Majumdar and P. Tabuada (Eds.): HSCC 2009, LNCS 5469, pp. 31–45, 2009. c Springer-Verlag Berlin Heidelberg 2009.

