International Journal of Technology Research and Management
ISSN (Online): 2348-9006
Vol 2 Issue 3 March 2015

A Novel Paradigm for the Assessment of Distributed Denial of Service Attack in Wireless Sensor Network

Megha Dubey[1], Prof. Mayank Bhatt[2], Prof Rajat Bhandari[3]
Research Scholar, Rishiraj Institute of Technology, indore[1]
Ast. Prof, Rishiraj Institute of Technology, indore[2]
Head of Department, Rishiraj Institute of Technology, indore[3]
dubeymegha14@gmail.com[1], mayankbhatt27@gmail.com[2], ritcsehod@gmail.com[3]

Abstract: *Mobile wireless sensor network is a subset of mobile ad hoc network. Therefore independent nods mobility is an essential property of network. The proposed routing protocol is implemented and simulated in NS2 network simulation environment. In order to simulate the routing performance using two different network scenarios the performance is compared. And the comparative performance study is performed in terms of packet delivery ratio, throughput, end to end delay and energy consumption. The obtained results demonstrate the effective performance with respect to the traditional routing protocol.*

Keywords: *DDOS attack, Security, Routing Protocols*

1. Introduction

A WSN is a shared real-time system. Dismally yet very little work is applied in these new system and always a new solutions are often essential in all areas of the scheme [1]. The main cause is that the set of assumptions underlying earlier work has changed dramatically. Most of the earlier distributed systems research works on the following assumption like the systems are wired; powers is unlimited, not works on real-time, with a fixed set of resources, have user consolidate such as display and mike, treat each node of the system as very significant and are location independent. In contrast, the designing of a wireless sensor network should be formulated with keeping following terms in consideration such as the systems is completely ad-hoc and works with wireless channel, have scarce power, are real-time, utilize the sensors and actuators as interfaces, with dynamically changing sets of resources, aggregate behaviour is also important there and location is very critical. Various wireless sensor networks also exploit negligible capability machines which places a more burden on the ability to usage precedent solutions.

In this proposed work the wireless sensor networks are investigated for their security and performance issues. Due to observations that is found that these are basically dependent on the routing strategy by which the network nodes are finding routes for delivery data, most of the attackers are take advantage of routing techniques are easily able to deploy the attacks in such kind of networks. There are significant amounts of routing based attacks are available but there are too fewer work is found for the Distributed DOS in wireless sensor networks. The further study is devoted to find an optimum solution for the Distributed DOS which causes the energy loss and performance losses in wireless sensor networks [2].

2. Background

This Literature survey provides the understanding about routing techniques and the different security issues in routing techniques. In addition of that Distributed DOS attack properties and their issues are also discussed in detail. Moreover it for finding an effective solution for Distributed DOS attack various recently developed approaches and techniques are also discussed in this section.

P. Rajipriyadharshini et al [15] provides a solution for Distributed DOS and described as Wireless sensor network is a communication network across the sensors nodes. Sensor nodes collect information about the physical environment. Now-a-days one main issue in wireless ad-hoc sensor network is wastage of energy at each sensor nodes. Energy is the one most important factor while considering sensor nodes.

B. Umakanth et al [16] consider how routing protocols, affects from attack even those create to be protect, lack security from these attacks,which we call Distributed DOS attack, which permanently disable networks by quickly draining vertex' battery power.

DOS flooding are not specify to any particular protocol, but rather rely on the properties of many popular classes of routing protocols. A single Distributed DOS attack can maximize network-wide energy usage by a factor of O(N), where N in the number of network vertex.

P.DivyaPrabha et al [17] will use two attack on stateless protocol in which first Carousel attack is an competitor broadcast a message with a path given series of loops, such that the same vertex display in the path more than one time. Second, Stretch attack where a nasty vertex create artificially long source routes, causing message to cut cross a bigger than best number of vertex. The Distributed DOS attack are very tough to determine and more over very difficult to secure.

3. Problem Domain

Wireless sensor network is a group of network devices known as vertex are connected with wireless connectivity called links. The availability of interconnection is given a specified range of radio range. Therefore for interaction each other the data is traveled through mediator nodes. The intermediate node selection for distribute the data is responsibility of routing algorithms. These routing algorithms are endeavor to search an optimum path between source and receiver. Therefore a vicious node can any time accompany the network and can damage the normal functioning of network.

4. Solution Overview

In this presented work a explanation for Distributed DOS Attack (resource consumption attack) in wireless sensor network environment is introduces. In this attack attacker nodes are behaving as normal behavior nodes. But by the network activity the nodes are consuming the network resources much frequently such as battery power, bandwidth. In addition of that sometimes these attackers misguiding the packets before delivery to target node by creating path loops. Thus detection of such malicious nodes in network is required. This presented work demonstrates a routing scheme with decisional threshold to detect the malicious acting nodes.

For implementing the desired scheme using the routing technique, the NS2 simulation environment is suggested for simulation. And for simulating the effect of improved routing technique AODV routing protocol is modified for implementing the security solution. The objective of proposed work is improve transmission periods of nodes via specifying minimum enduring efficiency of vertex to protect data transmission from irregular manner. A projected technique also extend to transmit set up data messages and eliminate Route Request messages appears from another vertex during regular communication. This work reduce battery dissociation along eliminating path discovery request messages and exxagerate a period of data transmission.

5. Simulation

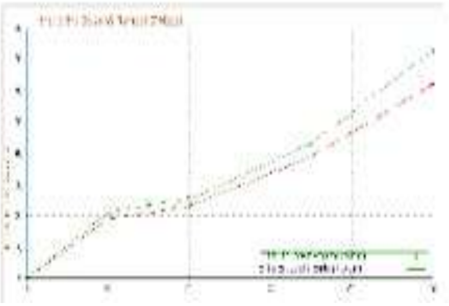
NS is a discrete event simulator directed at networking research. NS provides noteworthy support for simulation of routing, TCP, and multi cast protocols on wired and wireless networks. A simulator model of a real-world system is essentially a popularization of the real-world system self.

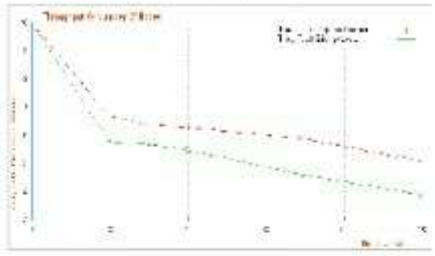
a. **Topology definition:** To simplicity in the creation of basic facilities and define their interrelationships.
b. **Model usage:** To simulate the network scenario required to added models to simulation (for instance,IPv4,UDP, point-to-point links and devices, applications); most of the time this is done using helpers.
c. **Node and link configuration:** Here simulation model uses their predefined values for instance, an application sends a particular size of packets or MTU of a point-to-point link frequently do this using the system attribute.
d. **Execution:** Simulation facilities generate events, data requested through the user is logged.

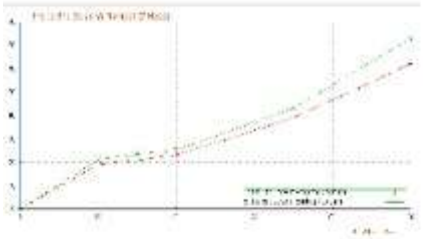
6. Result Analysis

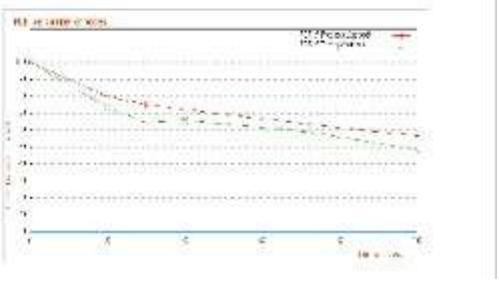
This section demonstrates the performance of the proposed routing protocol. In addition of that comparative performance study is provided with respect to the previously available technique for preventing Distributed DOS attack in wireless sensor network.

In this diagram the blue line shows the energy consumption during the proposed routing protocol and the red line shows the traditional routing node's life time. According to given figure the X axis demonstrate the number of nodes in the Network during the simulation scenarios and the amount of energy consumed is given by the Y axis in diagram in terms of Joules.









This Figure simulates the comparative packet delivery ratio during communication scenarios. Where the X axis shows the number of nodes in network and Y axis shows the amount of packets delivered in terms of percentage. In this diagram the X axis shows the number of nodes in network and the amount of end to end delay is given using Y axis.

7. Conclustion & Future Work

The wireless sensor network is one the popular networks in now these days, a rich amount of applications are designed using the help of wireless sensor networks management. Therefore a new solution is proposed for preventing the malicious nodes in network. The proposed solution first consumes the historical data for estimating decisional threshold for detection and prevention of Distributed DOS attack. The proposed routing protocol is an efficient and effective routing protocol, and able to detect malicious nodes in wireless sensor network. But the performance of proposed routing protocol is decreases as the number of network nodes are increase frequently.

In order to justify the proposed routing protocol's effectiveness the comparative performance study is performed with respect to the traditional available routing protocol. The performance of the proposed routing is adoptable due to high bandwidth availability, low energy consumption, higher packet delivery ratio and less end to end delay.

Acknowledgments

The author would like to thank Prof. Mayank Bhatt for his help. This work was supported in part by the RIT, Indore.

References

[1]. Anupama Sahu, Eduardo B. Fernandez, Mihaela Cardei and Michael VanHilst, "A Pattern for a Sensor Node", Department of Computer and Electrical Engineering and Computer Science Florida Atlantic University, Boca Raton, FL 33431

[2]. Archana Bharathidasan, Vijay Anand Sai Ponduru, "Sensor Networks: An Overview",

Department of Computer Science University of California, Davis, CA 95616.

[3]. Eugene Y. Vasserman and Nicholas Hopper, "DOS : Draining Life from Wireless Ad Hoc Sensor Networks", IEEE Transactions on mobile computing, Vol. 12, No. 2, February 2013

[4]. Th. Arampatzis, J. Lygeros, and S. Manesis, A Survey of Applications of Wireless Sensors and Wireless Sensor Networks, Proceedings of the 13th Mediterranean Conference on Control and Automation Limassol, Cyprus, June 27-29, 2005, 0-7803-8936-0/05/$20.00 ©2005 IEEE.

[5]. Luis Javier García Villalba, Ana Lucila Sandoval Orozco, Alicia Triviño Cabrera and Cláudia Jacy Barenco Abbas," Routing Protocols in Wireless Sensor Networks", Int.Journal of Sensors,Vol.9,pp. 8399-8421

[6]. K. Akkaya and M. Younis, "A Survey of Routing Protocols in Wireless Sensor Networks", in the Elsevier Ad Hoc Network Journal, Vol. 3/3 ,pp. 325-349, 2005

[7]. A. Abbasi, M. Younis, "A survey on clustering algorithms for wireless sensor networks, "in Elsevier Computer Networks Computer Communications, vol. 30,pp.2826-2841,October2007.

[8]. O. Younis, M. Krunz, S. Ramasubramanian, "Node clustering in wireless sensor networks: recent developments and deployment challenges," IEEE Network, vol. 20, pp. 20-25, May 2006.

[9]. G. Nivetha, "Energy Optimization Routing Techniques In Wireless Sensor Networks" ,Volume 2, Issue 7, July 2012.

[10]. Jamal N. Al-Karaki, Ahmed E. Kamal, "Routing techniques in wireless sensor networks: A Survey", IEEE wireless communications volume 11, pp.6-28, December2004.