ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

Prevention of DDOS Attack in Wireless sensor network using secure routing

Megha Dubey[1], Prof Mayank Bhatt[2], Prof Rajat Bhandari[3]

Research Scholar, Rishiraj Institute of Technology, Indore[1]

Assistant Professor, Rishiraj Institute of Technology, Indore[2]

Head of Department, Rishiraj Institute of Technology, Indore[3]

Abstract: Mobile wireless sensor network is a subset of mobile ad hoc network. Therefore independent nods mobility is an essential property of network. Due to limited radio range the communication is also performed in ad hoc manner. In these networks the routing protocol played important role in route discovery between communicating nodes. Due to this the network suffers from the performance issues. Among them security is main area of concern in the presented work. Therefore different routing based attacks are investigated and a serious resources consumption attack is addressed. This attack using false messaging, or by modifying routing information network performance is affected. Thus an improved routing solution is suggested. This paper is 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: DOS attack, flooding attack, Routing Protocols, Security

INTRODUCTION

Routing protocols specify the manner in which nodes and routers communicate and disseminate information. There are various issues that should be considered for routing in WSNs. Some of the issues are Energy Efficiency, Ad-hoc Deployment, and Prone to failures etc.. Since the WSNs are dynamic, the main task in routing is the identification of nodes. Once the nodes are identified the routing protocols are responsible for the construction and maintenance of the routes between nodes. There are several routing algorithms which are specifically for some applications. [5] Routing in WSNs can be categorized as flat-based routing, location-based routing, and hierarchical –based routing [5] [6]. This classification is done on the basis of network architecture. The flat based protocols all the vertex are assigned balanced functionality. In location based protocols the instruction about the situation is used to assign the data to wish for regions than to assign it to the full network. In hierarchical protocols clustering of the nodes is done in which bunch head is elected which implement some reduction and aggregation of data so as to recover energy. [7]

There are several expansion techniques used in path searching for WSNs. Some of them are: Attribute-based, Energy optimization, Data aggregation, Addressing schemes, Location-based, Multipath communication, quality of service etc. [5]. In the following section we will discuss about the approach of hierarchical routing.

for delivery data, most of the attackers are take advantage of routing techniques are conveniently able to deploy the attacks in such type of networks. There are significant amounts of routing based attacks are accessible but there are too fewer work is found for the DDOS in wireless sensor networks. The farther study is dedicated to find an optimum solution for the DDOS flooding which purpose the energy loss and performance losses in wireless sensor networks [2].

SECURITY ISSUES IN ROUTING

In wireless networks there are different kinds of routing based attack deployment issues are observed. Some of them most frequent attacks are listed in this section.

Passive Attack- A passive attack does not disturb the appropriate operation of the network. The malicious user snoops the data communicated in the network without modifying it. Here, the prerequisite of confidentiality can be dispelled if an attacker is also able to interpret the data gathered through snooping.

Active Attack- An active attack tries to modify or destroy the data being conveyed in the network, thereby disturbing the usual functioning of the network. It can be classified into two classes' external and internal attacks.

Wormhole attack- In a wormhole attack more than one malicious nodes are joining the network and according to the nodes they are connected thorough, high speed data buses by which their promises to send data from source to sink, the form of attack is determined as a malicious node can capture packets at one place in the network and tunnel them to another place through a private network pooled with a colluding malicious node.

Black hole attack- In this attack, an attacker uses the routing protocol to broadcast self as the shortest path to the node whose packets it wants to interrupt. An attacker hears the requests for routes in a flooding based protocol.

Byzantine Attack: In this attack, a compromised intermediary node or a set of intermediate nodes works in agreement and perform attacks like creating routing loops, dispatching packets on non-finest paths and selectively

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

falling packets which results in disturbance or degradation of the routing services.

Resource Consumption attack: In this attack, an attacker effort to consume or drain the resources of other devices available in the network. The resources that are aimed are bandwidth, battery power, and computational power, which are only available in limited amount in ad hoc wireless systems.

Rushing Attack: On-demand routing protocols that use identical conquest during the route discovery practice are susceptible to this attack. An attacker which receives a route request packet from the originating node floods the packet, rapidly throughout the network earlier other nodes, which also obtain the same route request packet, can react.

Denal of Service: In this type of attack, an attacker efforts to avert legitimate and authorized users of the services obtained by the network. A denial of service (DoS) attack can be deployed in many techniques.

BACKGROUND

This Literature survey provides the understanding about routing techniques and the different security issues in routing techniques. In addition of that vampire attack properties and their issues are also discussed in detail. Moreover it for finding an effective solution for vampire attack various recently developed approaches and techniques are also discussed in this section. Finally the concluding facts are listed for improving security in routing technique is also discussed.

2.1.1 Hierarchical routing –

It is also known as cluster based routing because the nodes are divided into clusters and a cluster head is elected by them. The communication happens through the cluster heads only.

2.1.2 LEACH (Low Energy Adaptive Clustering Hierarchy)

In this protocol the cluster head is periodically changed so that the energy consumption is equally distributed In LEACH, the cluster head nodes performs the compression of data arriving from nodes that belong to the respective cluster, and send a gross packet to the base station so that the amount of information that must be transmitted to the base station is reduced.

2.1.3 PEGASIS (Power-Efficient Gathering in Sensor Information Systems)

This is the augmented version of the LEACH protocol. In this protocol the chain of the sensor nodes is formed and nodes only communicate with their neighbour nodes so as to extend the network lifetime. Data is collected from the nodes and transferred to the node which communicates with the base station.

2.1.4 TEEN (Threshold Sensitive Energy Efficient Sensor Network Protocol)

TEEN is another hierarchical protocol for hyperactive networks that is those networks which responds immediately to changes in the given parameters. In this protocol a cluster head sends two threshold values a hard value and a soft value. The nodes are meant to sense their environment uninterruptedly.

2.1.5 Hybrid Energy Efficient Protocol (HEEP)

HEEP makes use of PEGASIS principle inside the clusters. In HEEP, a chain of nodes is formed within the same cluster dissipation. Each cluster head sends the collected data collected in the cluster to the BS through cluster heads neighbours.

2.1.6 Power Efficient and Adaptive Clustering Hierarchy (PEACH)

PEACH protocol for WSNs was introduced to minimize the energy consumption of each node, and maximize the network lifetime. In this protocol, formation of the cluster is done by overhearing characteristics of wireless communication to maintain an adaptive multi - level clustering and to prevent other overheads.

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.

SOLUTION OVERVIEW

In this presented work a explanation for vampire 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.

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 vampire 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

DOI 10.17148/IJARCCE.2015.4231

ISSN (Online) : 2278-1021
ISSN (Print) : 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 4, Issue 2, February 2015

ACKNOWLEDGMENT

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 flooding: 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.