MJRET
Open Access
Multidisciplinary Journal of Research in Engineering and Technology
Journal homepage: www.mjret.in
ISSN:2348 - 6953

VAMPIRE ATTACKS: DETECTION AND ELIMINATION OF DISHONEST NODES IN SENSOR NETWORKS

H.K.Chaudhari[#1], C.S.Jadhav[#2], M.S.Kalane[#3], V.K.Kulkarni[#4]
[#1234]Department of Computer Engineering, University of Pune
Imperial College Of Engineering and Research
Pune, India
[1]harshuc4@gmail.com, [2]chaitu0019@gmail.com,
[3]monikakalane@gmail.com,[4]vaibhavkulkarni1993@gmail.com

Abstract- *Wireless sensor networks are an exciting research direction in sensing with various parameters like security, energy. Most of the prior security work has done with denial of communication at the routing or medium access control levels. This paper mainly focuses on resource depletion attacks that is draining of battery life of the sensors at the routing protocol layer, which results in quickly draining nodes battery power. Vampire attacks do not have any architecture that is attacks are not specific to any specific protocol. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O(N), where N in the number of network nodes. In this paper, we are proposing two main modules, Analyzer and classifier which identify attacks on both stateless and stateful protocol and avoid the damage caused by dishonest or called vampire nodes during the packet forwarding phase.*

Keywords-*protocol,security,routing,sensor networks,Denial of service.*

I. INTRODUCTION

Over the last couple of years wireless communication has become of such fundamental importance. Because of the established technologies such as mobile phones and WLAN, new approaches to wireless communication are emerging. The purpose of this to specify the requirements for building secure architecture for avoiding vampire attack and maximizing the endurance of the network through minimizing the energy.

We are representing functioning of designed architecture by developing web service and deploying it on that cloud. The module to be developed is the first version, i.e. version 1.0. Software Requirements Specification provides a complete description of all the functions and specifications of security architecture, version 1.0.

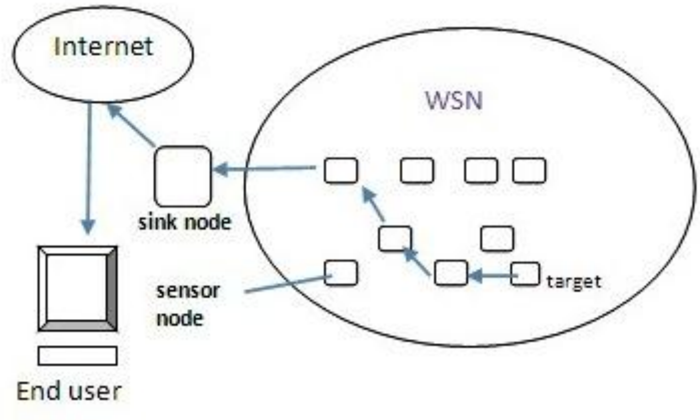

Fig. 1 Wireless Sensor Network

Over the last couple of years wireless communication has become of such fundamental importance as mobile phones and WLAN, new approaches to wireless communication are emerging; one of them are so called ad hoc and sensor networks. Ad hoc and sensor networks are formed by autonomous nodes communicating via radio without any additional backbone infrastructure. In recent years, Wireless sensor network (WSNs) plays a vital role in various application domains such as object detecting, medical caring, forest monitoring and so on. Energy's ability and scalability are two greater challenges in Wireless Sensor Networks.

2. LITERATURE SURVEY

2.1 Power Consumption in Wireless Sensor Networks[1]

In this paper author proposed that to increase sensor node's endurance, bounds and protocols have to be energy efficient so that they can make a priority reactions by estimating and predicting energy consumption. The Authors present and discuss several strategies such as potential-appraised protocols, cross-layer optimization, and accumalation technologies used to alleviate potential consumption constraint in WSNs.

Author states that to increase sensor node's endurance, integration of accumalation technologies and energy-appraised architecture and protocols are mandatory. This paper surveys the main approaches to energy conservation in WSN.

2.2 *Optimal Energy Consumption for Wireless Sensor Networks*[2]

In this paper, the author proposed a topology control method based on clustering, and used simulated Annealing to optimize energy saving in wireless sensor networks. Experiments show that the proposed method is able to average the energy consumption of sensor nodes, lengthen the endurance of each sensor node, prolong network endurance, and optimize data volume transmission of the whole system.

Due to congenital restriction of sensors, it is always a crucial issue on how to utilize limited energy effectively. Author first implemented a network topology construction method which is based on energy saving, which includes cluster forming and selecting middle heads and cluster heads.

2.3 Analysis of Energy Consumption and Lifetime of Heterogeneous Wireless Sensor Networks[3]

This paper examines the performance as well as energy consumption issues of a wireless sensor network providing periodic data from a sensing field to a remotely deployed receiver.

Author formulates the energy consumption and study their Estimated endurance based on a clustering mechanism with varying parameters related to the sensing field for example distance and energy level. Author quantified the optimal number of clusters based on proposed model and showed how to allocate energy between different layer.

3. PROPOSED ARCHITECTURE

Sensor networks are formed by autonomous nodes communicating via radio without any additional backbone infrastructure. Wireless Sensor Network (WSN) refers to a group of spatially distributed and devoted sensors for controlling and recording the physical conditions of the environment and arranging the collected data at a main fundamental locus.

The safeguarding tracts that are required by sensor networks can be categorized as:-

a) Data Privacy:- A sensor network should preserve the data from the networks collegial to it. The result of the problem can be achieved by data encryption

b) Data Attestation:-The data needs to be authenticated for the data originating from an authenticated source and not from a malicious source. It is achieved through parallel symmetric mechanism. But we need authenticated broadcast mechanism and hence we create an asymmetric mechanism from symmetric primitives.

c) Data Uprightness:- This is required to check whether the receiver has received the data that not been modified in course.

Wireless sensor network has experienced massive growth in the corporate industry throughout the past several years, especially as the technology caters to data sensing and accessibility

So, our objective is to build a security service which will detect vampire nodes and remove from the network by avoiding vampire attack and maximizing the lifetime of the network through minimizing the energy. We are representing functioning of designed architecture by developing web service and deploying it on that cloud.

We are going to perform following, for detection and prevention of vampire attack:-

1. To construct vampire node detection system which would provide node verification will defined in node analyzing system.
2. Defining parameter list for classifying honest node and vampire node.
3. To construct analyzer for packet routing from each sensor.

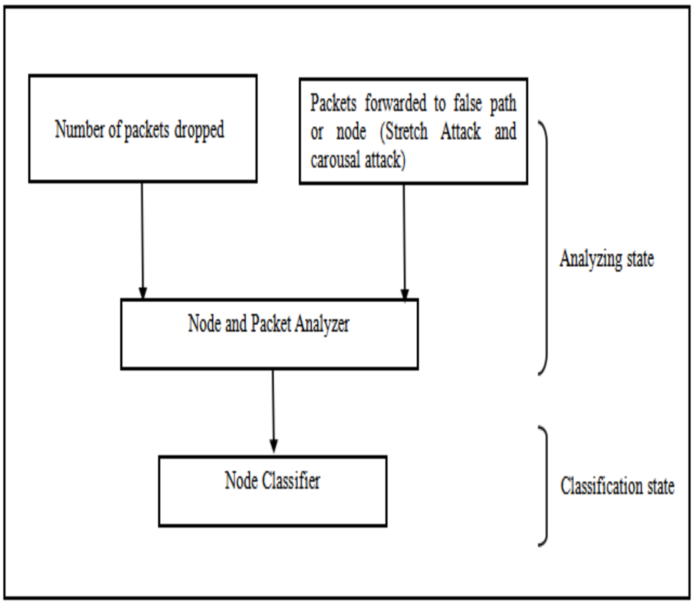
Number of packets dropped
Packets forwarded to false path or node (Stretch Attack and carousal attack)
Analyzing state
Node and Packet Analyzer
Node Classifier
Classification state

Fig. 2 Analyzer and classifier Architecture Diagram

The Architecture shows two main modules analyzer and classifier.Analyzer module analyzes every node in network with some parameters like number of packets dropped by particular node or number of packets sent to the false path and classifier classifies honest and vampire node with the help of result calculated by analyzer node.

4. ADVANTAGES OF PROPOSED SYSTEM

1) Proposed system classifies the node based on analysis.
2) Protect from vampire attacks.

3) Secure level is high.
4) After detecting vampire node system track his location and remove attacker node from network.
5) Boots up the battery potential.

5. DISADVANTAGES OF PROPOSED SYSTEM

System cannot determine whether the attack is insider attack or outsider attack so it is necessary to provide digital signature to every sensor to verify whether that sensor belongs to particular network or not, and it will be the extension of proposed system.

6. CONCLUSION

This paper mainly focuses on resource depletion attacks that is draining of battery life of sensors at the routing protocol layer, which results into quickly draining nodes battery potential. These attacks are not dependent on any particular protocols.Proposed system comprises two main states analyzing state and classification state. Analyzer state analyzes every node in network with some parameters like number of packets dropped by particular node or number of packets sent to the false path and classifier perform filtering and classify node as honest or vampire node.Wireless sensor networks promise exciting new applications in the near future. As WSN's become more and more crucial to everyday life so it is important to implement and also improve security mechanism for various attacks.

ACKNOWLEDGMENT
We would like to sincerely thank Mr. Rokade, our guide, for his support and encouragement.

REFERENCES

[1] *Power Consumption in Wireless Sensor Networks Sidra Aslam Punjab University College of Information Technology (PUCIT) University of the Punjab Allama Iqbal (Old) Campus, Anarkali, Lahore, Pakistan +92-(0)42-111-923-923 sidra.aslam@pucit.edu.pk Farrah Farooq Punjab University College of Information Technology (PUCIT) University of the Punjab Allama Iqbal (Old) Campus, Anarkali, Lahore, Pakistan +92-(0)42-111-923-923 farrah.farooq@pucit.edu.pk Shahzad Sarwar Punjab University College of Information Technology (PUCIT) University of the Punjab Allama Iqbal (Old) Campus, Anarkali, Lahore, Pakistan +92-(0)42-111-923-923-414 s.sarwar@pucit.edu.pk*

[2] *Optimal Information Extraction in Energy-Limited Wireless Sensor NetworksFernando Ord´ o˜nez1 and Bhaskar Krishnamachari2 1 Department of Industrial and Systems Engineering, 2Department of Electrical Engineering, University of Southern California, Los Angeles, CA 90036, USA {fordon, bkrishna}@usc.ed*

[3] *Analysis of Energy Consumption and Lifetime of Heterogeneous Wireless Sensor NetworksEnrique J. Duarte-Melo, Mingyan Liu EECS, University of Michigan, Ann Arborejd, mingyan@eecs.umich.edu*

*[4] SidraAslam,FarrahFarooq,ShahzadSarwar,"***potential*** Consumption in Wireless Sensor Networks",March 2012.*

[5] Jang, Hung-Chin Lee, Hon-Chung Huang, Jun-Xiang,Department of Computer Science National ChengChi University, Taiwan, R.O.C."Optimal Energy Consumption for Wireless Sensor Networks".

[6] Enrique J. Duarte-Melo, Mingyan Liu EECS, University of Michigan, Ann Arbor"Analysis of Energy Consumption and Lifetime of Heterogeneos Wireless Sensor Networks".

[7] Ismail Butun, Salvatore D. Morgera, and Ravi Sankar,ATIONS SURVEYS & TUTORIALS, VOL. 16, NO. 1, FIRST QUARTER 2014,"A Survey of Intrusion Detection Systems in Wireless Sensor Networks"

[8] http://www.notforme.kr/archives/963