ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (179-183), Month: April - June 2015, Available at: www.researchpublish.com

Vampire Attacks: "Intrusion Detection and Efficient Use of Sensor Nodes"

[1]Vaibhav kulkarni, [2]Monika Kalane ,[3]Chaitali Jadhav,[4]Harshada Chaudhari, [5]Prof.D.N.Gadekar

[1, 2,3,4,5] Savitribai Phule University of Pune, Imperial College of Engineering and Research, India

Abstract: **In the recent years ad-hoc sensor networks are used widely in various aspects and has a wide area of application, the scope of wireless ad-hoc sensor network lies widely in its security and the way the data is transferred, in this paper we will implementing various parameters in order to make secure the wireless sensor networks from vampire attacks, which are not protocol specific ,also catapulted various protocols in order to increase the efficiency of sensor nodes battery and the comparison of graphs depict how efficient our implementation is as compared to previous research, also the protocols used are used to make the wireless sensor network robust and the optimized use of sensor nodes battery. We will also be analyzing the causes and effect causing vampire attack and depletion of sensor nodes battery and preventive measures accomplishing our objective, the graph analysis clearly portray our prominent work as compared to previous articles as less energy consumption thus maximizing the performance of sensors.**

Keywords: **Protocol, Disparaging, Adversaries, Data Sequestration/Concealment, Data, Substantiation/Corroboration, Data Perpendicularity, Depletion attack**

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 avenues 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 disparaging the energy.

We are representing functioning of designed architecture by developing web service and deploying it on that cloud. The calibre/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.

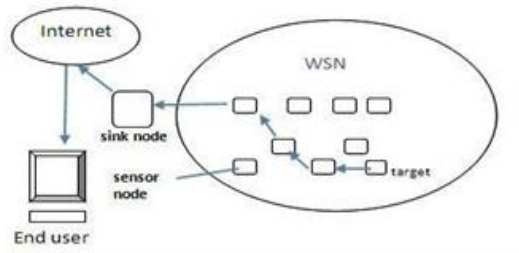

Fig. 1 Wireless Sensor Network

Over the last couple of years wireless communication has become of such fundamental importance as mobile phones and WLAN, new assesions 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 framework. 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 Efficient Detection and removal of vampire attacks in wireless ad-hoc sensor networks:

In this paper author showed that the attack does not depend on particular protocol also author showed a proof of concept of attacks against representative examples of existing routing protocols using small number of weak adversaries, and measured their attack success on randomly generated topology of 30 nodes. Simulation results showed that depending on the location of adversary, Network energy expenditure of the following phases, increases from 50 to 1000 per cent

2.2 ***Overcome Vampire Attacks Problem in wireless ad-hoc sensor network by using distance vector protocols:***

In this paper author presents vampire attack a new class of resource consumption attack that uses routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes battery power. Here depending on the location of the adversary, network energy expenditure during the forwarding phase increases drastically. The proposed technique routing protocol are provably bounds damage from vampire attacks by verifying that packets consistently make progress toward their destinations and reduce the reimbursement.

2.3 Analysis of Energy Consumption and Lifetime of Heterogeneous Wireless Sensor Networks:

This papery scrutinizes 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 calibrated 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 groundwork. 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 bulwarking tracts that are required by sensor networks can be categorized as:-

a) Data Sequestration/Concealment: 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 Substantiation/Corroboration: The data needs to be authenticated for the data originating from an authenticated source and not from a detrimental inception

It is achieved through parallel commensurate mechanism. But we need authenticated broadcast mechanism and hence we create a commensurate mechanism from commensurate primitives.

c) Data Perpandicularity: 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:-

To construct vampire node detection system which would provide node verification will defined in node analyzing system.

1. Defining parameter list for classifying honest node and vampire node.
2. To construct analyzer for packet routing from each sensor.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (179-183), Month: April - June 2015, Available at: www.researchpublish.com

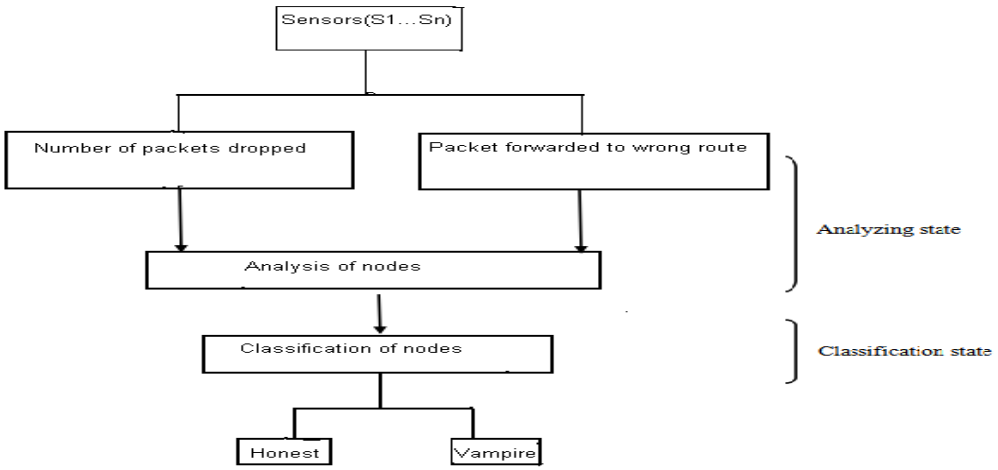

Fig. 2 Analyser and classifier Architecture Diagram

The Architecture shows two main modules analyser and classifier. Analyzer module analyses 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 analyser node.

4. RESULTS

In this section we proposed the analysed results of algorithm and compared results with existing algorithms

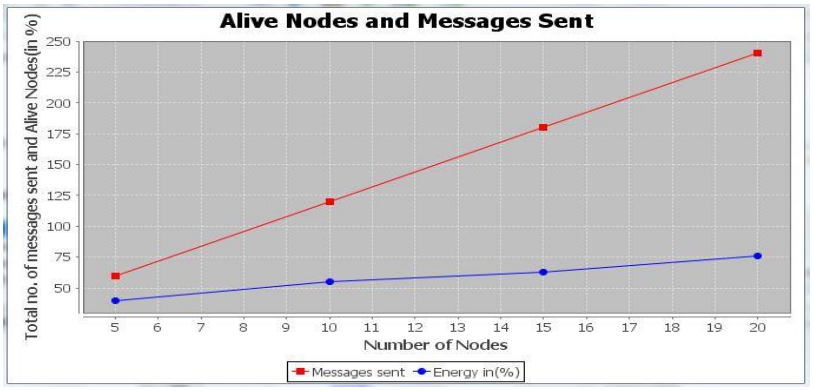

Fig. 4.1 Graph

Graph 4.1 shows the graph of number of messages sent verses alive node or energy remained. Firstly when number of nodes is 5 and messages sent by those 5 nodes are 60 then energy remained will be 30 per cent as well as when messages sent by 20 nodes are 240 then energy of network will be 75 per cent.

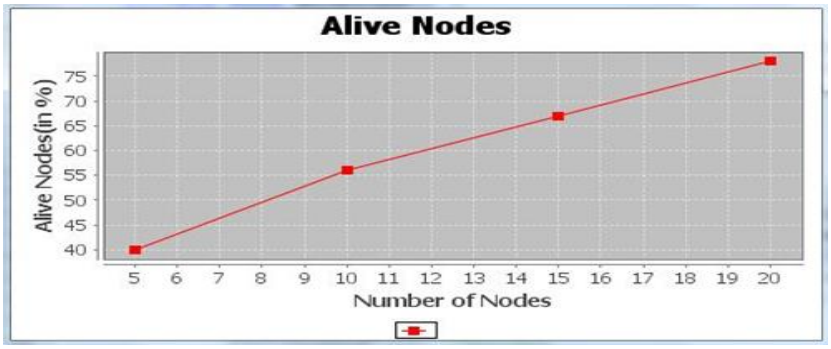

Fig. 4.2 Graph

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 3, Issue 2, pp: (179-183), Month: April - June 2015, Available at: www.researchpublish.com

Graph 4.2 shows the direct proportionality between number of increasing nodes verses number of alive nodes that is more the number of nodes in the network more will be the alive nodes remained in network.

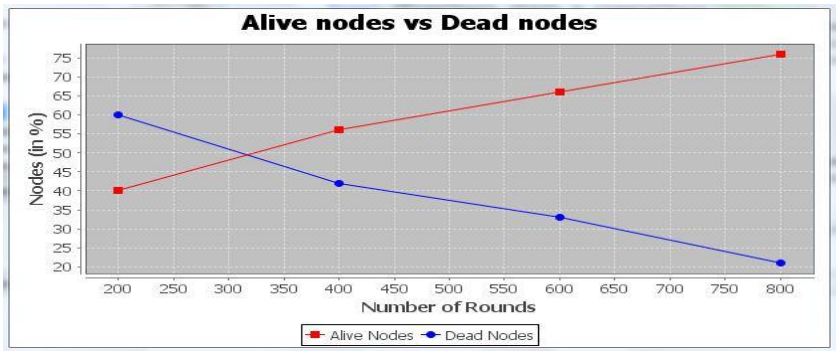

Fig.4.3 Graph

Graph 4.3 shows the number of alive nodes and dead nodes remained after each round. Initially when number of rounds are 200 the percentage of alive nodes less than percentage of dead nodes. When number of nodes are 800 then percentage of alive nodes are more than the percentage of dead nodes.

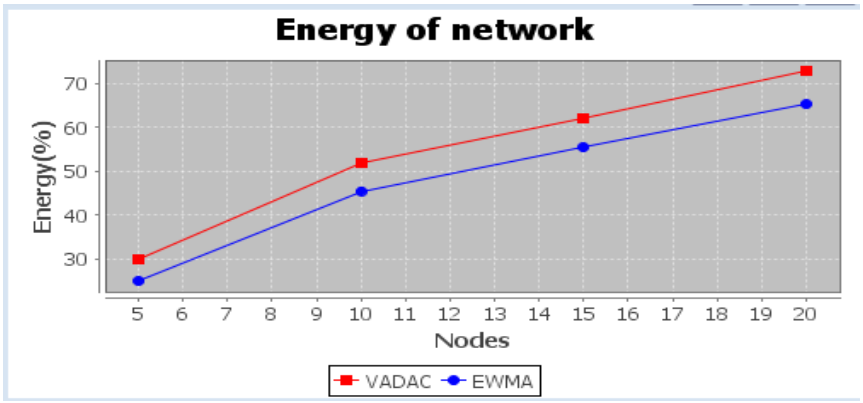

Fig.4.4 Graph

Graph 4.4 shows the energy saved by proposed algorithm that is Vampire attack detection using analyser and classifier (VADAC). And EWMA which shows that proposed algorithm saves more energy than EWMA.

5. 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.

6. DISADVANTAGES OF PROPOSED SYSTEM

System cannot Ordain whether the attack is conspirator attack or intruder 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.

7. CONCLUSION

This paper mainly focuses on resource depletion attacks that are draining of battery life of sensors at the routing protocol layer, which results into expeditiously sapping nodes battery potential. These attacks are not dependent on any particular protocols. Proposed system comprise two main quandaries: analysing state and classification state. Analyser state analyses 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 affiance bracing new applications in the adjoining prospective. As WSN's become more and augmented pivotal to everyday life so it is important to implement and also improve security mechanism for various attacks.
Our paper correlated with other paper proves how efficient is our algorithm and the salvation of node's battery for greater consummation/performance

8. ACKNOWLEDGEMENT

I express my sincere respect and gratitude to my guide Prof. Devendra Gadekar who has given valuable support cooperation and suggestions from time to time in successfully completing this project work.

REFERENCES

[1] Power Consumption in Wireless Sensor Networks Sidra Aslam Punjab University College of Information Technology (PUCIT) University of the Punjab AllamaIqbal (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 AllamaIqbal (Old) Campus, Anarkali, Lahore, Pakistan +92-(0)42-111-923-923 farrah.farooq@pucit.edu.pk ShahzadSarwar Punjab University College of Information Technology (PUCIT) University of the Punjab AllamaIqbal (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 NetworksFernandoOrd´ 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 Networks Enrique 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 Heterogeneous 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