International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395 -0056
Volume: 03 Issue: 09 | Sep-2016 www.irjet.net p-ISSN: 2395-0072

Time Based Detection and Prevention of Vampire Attacks in Wireless Sensor Network

Harpreet Kaur[1], Jasmeet Singh Gurm[2],

[1]*Harpreet Kaur*
Research scholor

Department of computer science and Engineering RIMT university, Fatehgarh Sahib, Punjab, india

[2]Jasmeet Singh Gurm
Assistant professor

Department of computer science and Engineering RIMT university, Fatehgarh Sahib, Punjab, india

---

Abstract - *Wireless sensor network is a communication network across the sensors nodes. A sensor node collects information about the physical environment. In Wireless Sensor Network, we focus on the Vampire Attacks. The vampire Attack is the resource depletion Attack at layer of network to reducing the battery power of any node. In this paper of Time based detection and prevention of Vampire Attacks in WSN, we focus on Carousel attack and Stretch attacks. Our proposed scheme aims to detecting the malicious attackers and then preventing them from taking part in the communication process. An algorithm is proposed to detect and prevent such attacks from draining energy of the nodes. The performance of the network has been analyzed on the basis of packet delivery ratio, throughput, and energy consumption.*

Key Words: Wireless Sensor Network, Vampire Attack, Carousel Attack, Stretch Attack, Packet Delivery Ratio, Throughput.

1.INTRODUCTION

The continuous evolutions in Micro Electro-mechanical systems (MEMS) and wireless communications have given rise to wireless sensor networks as the modern day technology .Wireless sensor networks are gaining potential focus they are provided as the low cost solutions to a variety of real-world challenges. Their low cost facilitates the deployment of large sensor arrays in a numerous circumstances capable of performing both military and civilian tasks. Sensor node is a smart, tiny, self-organizing low cost multi-functional device, containing battery, radio communication, microcontroller and sensors. It has exceptionally constrained processing capacity, battery force, and memory furthermore a limited field of sensing. A wireless sensor network (WSN) is a wireless network comprising of countless spatially disseminated sensor nodes. These sensor hubs can be effortlessly sent at vital regions requiring little to no effort. Containing various kinds of sensors, sensor nodes participate with each other to address the physical or environmental conditions, including temperature, sound, image, vibration, pressure, motion or pollutants.

1.1 VAMPIRE ATTACK

The vampire attack is the resource depletion attacks because that attack the network features like power, bandwidth, and energy consumption and the routing depletion attacks usually only affect the routing path. These attacks are known as "Vampire attacks" because they drain the battery power from the nodes. They do not affect a single node they take their time attack one by one and disrupt the entire system. The strength of the attack is measured by the ratio of network energy used in the benign case to the energy used in the malicious case. Mainly there are two types of vampire attacks, carousel attack and stretch attack.

1.Carousel attack As shown in Fig.1, in this attack, an adversary sends a packet with a route which is the series of loops, such that the same node shows in the route many times. It increases the route length beyond the number of nodes in the network, which is limited by the number of allowed entries in the source route.

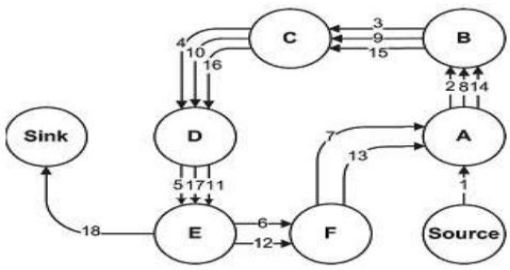


Fig1. Carousel attack

2. Stretch attack As shown in Fig.2, in stretch attack, attacked node constructs artificially long source path. Because of that packets traverse more number of nodes in network than optimal number of nodes. The original route is

S→J→D, which affecting four nodes including itself, but the attacked node selects a longer route i.e. S→A→B→C→ E → F→G→H→I→J→D, and make packet to traverse through more nodes in the network. These routes cause nodes that do not consist in the original route to consume energy by forwarding packets.

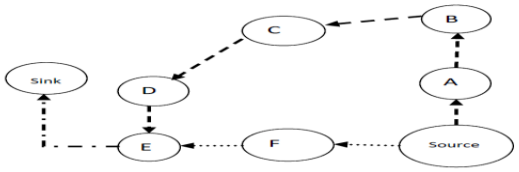


Fig.2 Stretch attack

2. LITERATURE SURVEY

In 2015 Amee A. Patel, Sunil J. Soni [1] Authors proposed the method prevents the draining of life from network nodes in wireless sensor networks .This paper works on the threshold energy of node. The problem of vampire attack can be reduced to some extent .The main purpose of this paper use some routing protocols for energy draining.

In 2014 GayaThri Deyi, Nanda Kumar, Varalakshmi [2] Author's use reference point imparting mechanism (RPIM) to represent data gathering technique in order to minimize the energy consumption and end to end delay in wireless sensor network. This technique used to minimize the frequent energy drain among the sensor nodes for increasing lifetime of the network.In this paper the end to end delay is reduced by 84.42%.

In 2014 P.T. Kalaivaani, A.Rajeswari, [3] Author's purposed a scheme, Gang attack based energy efficiency scheme to achieve reliability, high en-routing filtering probability for better energy ,workload, meantime, minimized delay at a given time interval. This paper focus on minimize the energy wastage and reduce the false data injection at sink node which drops the packets at node level and in the sink level.

In 2015 G. Escudero Andreu ,K.G.Kyriakopoulos, F.J. Aparicio-Navarro and D.J. Parish, D. Santoro, M. Vadursi [4] focus on the problem of identifying virtual jamming attacks on IEEE 802.11 networks and give solution based on DS theory for detecting NAV attacks.

In 2015 Abdullah Akbar, S. Mahaboob Basha, Syed Abdul Sattar [5] Author's propose a scheme, a novel scheme based on Hellinger distance to detect low-rate and multi-attribute DDos attacks. The SIP load balancer to fight against DDos and detect DDos attacks by using load balancing features.

In 2015 Lina R.Deshmukh, A. D. Potgantwar [6] Author's use routing protocols for vampire attacks to completely deactivate ad hoc wireless sensor networks by reducing battery life of nodes. The authors discuss a new proof-of concept protocol for many type of attacks. This protocol reduced the damage caused at the time of packet forwarding by Vampires.

In 2014 Bi Jiana, E Xu [7] This paper proposed a ARMA-based traffic attack detection protocol and linear prediction technique for energy saving to protect sensor nodes from traffic attack.The author's use different monitoring schemes for different kinds of nodes.

In 2014 Su Man Nam, Tae Ho Cho [8] This paper focus on genetic algorithm-based PVFS to select effective verification CHs before transmitting the reports from a source CH in wireless sensor networks.This technique save energy approximate 10%.

In 2014 Quentin MONNET, Lynda MOKDAD, Jalel BEN-OTHMAN [9] Author's use the *cNodes* in clustered wireless sensor networks to monitor traffic of the nodes and to detect denial of service attacks and also provide a better load balancing in the cluster. This paper focus on energy balancing method to detect denial of service attacks in wireless sensor networks.

In 2014 E.Mariyappan, Mr.C.Balakrishnan [10] This paper presented a sensor network encryption protocol such as routing table and network address for each node dynamically using technique to maintain the network availability and forward a packet from sources to destination through intermediate node for preventing the power draining of sensor node even in the face of vampire attacks.

In 2014 Mrs. R.Abirami, Mrs.G.Premalatha [11] Author's use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes battery power .This paper also defined Vampire attacks of resource consumption attacks in wireless sensor networks .The author propose Interior Gateway Routing Protocol (IGRP) where router used to exchange routing data within an independent system.

In 2013 Eugene Y. Vasserman and Nicholas Hopper [12] Author's use the routing protocol for permanently disable ad hoc wireless sensor networks.This paper also include a proof-of-concept protocol that focus on the damage caused by Vampires during the packet forwarding phase.

3. PROBLEM FORMULATION

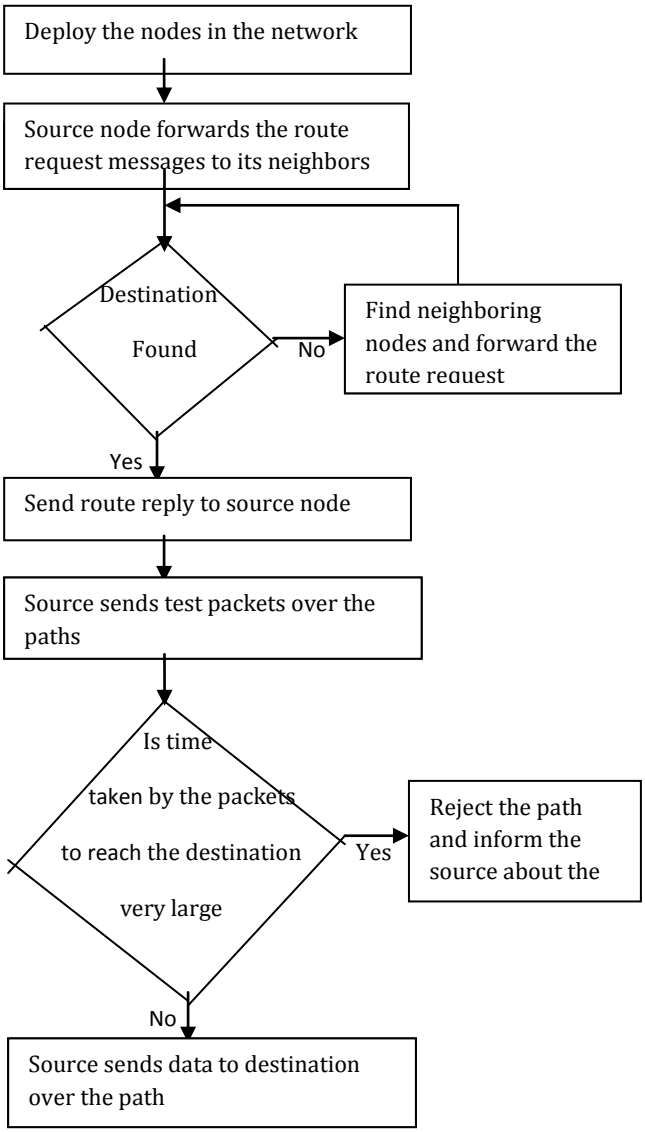
The vampire attack is the resource depletion attacks because that attack the network features like power, bandwidth, and energy consumption and the routing depletion attacks usually only affect the routing path. These attacks are known as "Vampire attacks" because they drain the battery power from the nodes. They do not affect a single node they take their time attack one by one and disrupt the entire system.

In the existing scheme [1] the nodes do not take the next nodes into path if their energy is less than some threshold value. In vampire attacks, the energy of the nodes will reduce once the attacker has been successful in forming the long route and has consume up energy of the nodes. This technique is however not a reactive one which detects the vampire attacks at early stages of the network.

4. PROPOSED SCHEME

In order to save energy of the sensor networks from being consumed due to vampire attacks, our proposed scheme aims at detecting the malicious attackers and then preventing them from taking part in the communication process. In our proposed scheme Source node will send the Route Request messages to find a route to destination node. Upon receiving the route request, the destination node will reply back to the source node via multiple paths. The source node will first send few test packets over the paths where the reply was received.

Proposed Algorithm:



5. CONCLUSIONS

In this paper, the proposed scheme relies on the time taken by the packets to reach the destination node to detect the attack. This does not require any extra amount of energy being consumed by the nodes. . The purposed scheme will be implemented in NS2.35 and analysed on the basis of parameters. These two parameters namely packet delivery ratio and throughput. This paper concluded time based detection of the vampire attack is efficient than energy based detection since the performance of the network had increased. In future however the proposed scheme can be analyzed against multiple attacker nodes in the network. Also the cryptographic measure can be added along with proposed scheme to make it more secure.

REFERENCES

[1] Amee A. Patel, Sunil J. Soni," A Novel Proposal for Defending Against Vampire Attack in WSN" Fifth International Conference on Communication Systems and Network Technologies, 2015.

[2] GayaThri Deyi, Nanda Kumar, Varalakshmi," A New Energy Consumption Technique in Wireless Sensor Network using Rrference Point and Imparting Mechanism" International Conference on Electronics and Communication System (JCECS), 2014.

[3] P.T. Kalaivaani, A.Rajeswari,"Impact of Gang Attack on Energy Efficiency Performance in Wireless Sensor Networks using Spatial Correlation Method" 2014.

[4] G. Escudero-Andreu, K.G. Kyriakopoulos, F.J. Aparicio-Navarro and D.J. Parish, D. Santoro, M. Vadursi," A Data Fusion Technique to Detect Wireless Network Virtual Jamming Attacks" Instrumentation and Measurement Society prior to the acceptance and publication, 2015.

[5] Abdullah Akbar, S. Mahaboob Basha, Syed Abdul Sattar," Leveraging the SIP Load balancer to detect and mitigate DDos attacks" International Conference on Green Computing and Internet of Things (ICGCIoT), 2015.

[6] 2015 Lina R.Deshmukh, A. D. Potgantwar," Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops" International Advance Computing Conference (IACC), 2015.

[7]Bi Jiana, E Xu,"A Safe and Energy-saving Traffic Attack Detection Protocol for WSN" Workshop on Advanced Research and Technology in Industry Applications (WARTIA), 2014.

[8] Su Man Nam, Tae Ho Cho," Improvement of Energy Consumption and Detection Power for PVFS in Wireless

Sensor Networks" Seventh International Conference on Mobile Computing, 2014.

[9] Quentin MONNET, Lynda MOKDAD, Jalel BEN-OTHMAN, "Energy-balancing method to detect denial of service attacks in wireless sensor networks" International Conference on Communication, 2014.

[10] E.Mariyappan, Mr.C.Balakrishnan," Power Draining Prevention In Ad-Hoc Sensor Networks Using Sensor Network Encryption Protocol" International Conference on Information Communication and Embedded Systems (*ICICES),* 2014.

[11] Mrs.R.Abirami, Mrs.G.Premalatha," Depletion of Vampire Attacks in Medium Access Control Level using Interior Gateway Routing Protocol" International Conference on Information Communication and Embedded Systems (*ICICES*), 2014.

[12] Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE Circuits and Systems, 2013.