International Journal of Scientific Research in Computer Science, Engineering and Information Technology
ISSN : 2456-3307 (www.ijsrcseit.com)
doi : https://doi.org/10.32628/CSEIT2390135

Detection of Vampire Attacks in Ad-Hoc Wireless Sensor Network using PLGP protocol

Gaurav Kawde[1], Safal Prabhukhanolkar[1], Shrinivas Tonpewar[1], Kushagra Belorkar[1], Shyam Kumar Patle[1], Chandu Vaidya[2]

[1]BE Scholar, Department of Computer Science Engineering, Rajiv Gandhi College of Engineering and Research, Hingna, Nagpur, Maharashtra, India

[2]Professor, Department of Computer Science Engineering, Rajiv Gandhi College of Engineering and Research, Hingna, Nagpur, Maharashtra, India

ABSTRACT

Article Info

Publication Issue :
Volume 9, Issue 1
January-February-2023

Page Number : 195-199

Article History
Accepted: 01 Feb 2023
Published: 16 Feb 2023

Wireless networks are an ideal research direction in the areas of sensors and pervasive computing. Wireless ad-hoc sensor networks are a new platform in the fields of remote sensing, data collection, analysis, problem solving, and various research studies. They contain nodes that act as transmitters and receivers, and are vulnerable to various attacks and incur various types of loss. Resource exhaustion attacks, once considered just a routing problem, now fall into a new group called "vampire attacks." A resource exhaustion or vampire attack drains a node's batteries, rendering them useless. Vampire attacks are not specific protocols and are hard to spot. This paper examines the identification and protection of resource exhaustion attacks at the routing protocol layer using the PLGP protocols (Parno, Luk, Gaustad, and Perrig). This white paper focuses primarily on detecting and preventing vampire attacks.

The proposed method is used to prevent network node exhaustion. This greatly reduces the problem of vampire attacks.

Keywords : Vampire attack, Wireless Ad-Hoc network, power drainage, PLGP, Wireless Sensor Network, Denial of service, Resource depletion ,Routing ,Energy consumption

I. INTRODUCTION

Sensor Sensor networks offer commercially viable solutions for a variety of applications, including critical infrastructure monitoring, security monitoring, and many medical applications [1]. As sensor networks are increasingly deployed in such safety-critical environments, the need for secure communication primitives is self-evident

Similarly, the development of such primitives facilitates the use of sensor networks in a wider range of applications. A central goal of this work is to ensure inter-node messaging even when the sensor network is actively attacked [2]. Maintaining correct routing information in the presence of an attacker is a very difficult task. An attacker could inject malicious routing information or modify routing configuration/update messages from legitimate nodes. Even if the route configuration/update messages are authenticated, the compromised sensor node itself could provide bogus routing information and cripple the Routing infrastructure. A WSN consists of nodes that do not have independent infrastructure. A WSN node consists of a data acquisition unit, a data transmission unit, and a processing unit, as shown in Figure 1. These nodes are used in different areas to gather information in different ways. Ad hoc wireless sensor networks (WSNs) promise ready-to-deploy communications. A "vampire" attack robs a network node of life. This project investigates resource exhaustion attacks against the routing protocol layer. This system is intended to be a fully functional network-based database system. Protects nodes from vampire attacks. It also improves battery performance due to his clean state sensor routing and his three main contributions. To avoid vampire attacks and save battery power, use Clean Slate Sensor Routing by Parno et al., Luk, Gaustad, and Perrig, also known as PLGP protocol. Base stations are typically orders of magnitude more powerful than sensor nodes [3]. They may have workstation or laptop-class processors, memory and storage, AC power, and high-bandwidth connections to communicate with each other.

However, sensors are limited to using low-power, low-bandwidth, short-range radios, so it is envisioned that sensor nodes will form a multi-hop wireless network to allow sensors to communicate with the nearest base station. It has been. A base station may require a steady stream of data. B. A sensor that reads every second from a node that can fulfill the request [4]. We call such a stream a data flow, and we call the node sending the data source. To save energy by reducing the total number of messages sent, sensor readings from multiple nodes can be processed at one of many possible aggregation points. A focal point collects sensor readings from surrounding nodes and forwards a single message representing the collection of readings.

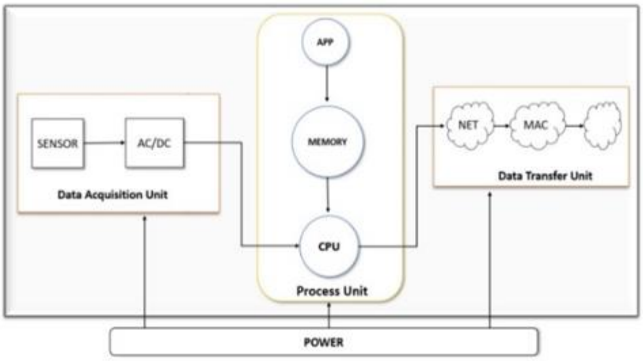

Fig 1. Nodes Of WSN

Aggregation points [5] are typically regular sensor nodes and their selection is not necessarily static. Aggregation points can be dynamically selected per query or event.

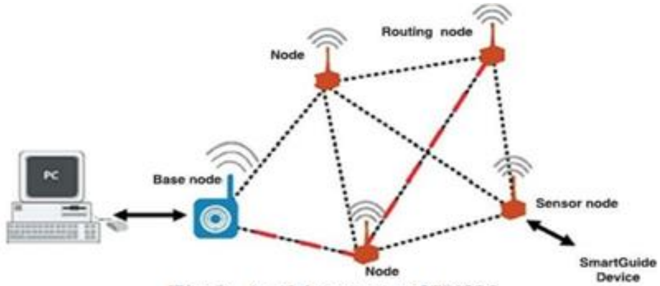

Fig 2. Architecture of WSN

Figure 2 shows the basic architecture of WSN [6]. It contains a number of nodes that act as routing nodes, sensing nodes, and base nodes. Figure 2 shows the architecture of WSN showing all the different types of nodes. Each node in the network can also act as an aggregation point and delay sending outbound messages until a sufficient number of inbound messages have been received and aggregated. Energy management in sensor networks is very important.

II. PROBLEM STATEMENT

Problem statement

The vampire attack is a serious problem in wireless sensor networks. Detection of these attack is very difficult. [7] The work has been done in the area of detection of vampire attacks on Wireless Sensor networks using PLGP protocol. [8] The work has been also done on detection and protection but they had concentrated on network layer and on application layer [9] but there is a chances to improvement so we have redefined the depletion attacks at all five layers 1) Physical layer 2) Data link layer 3) Network layer 4) Transport layer 5) Application layer using PLGP protocols. It will be very crucial in many of the situations and will increase the wide acceptability of adhoc wireless networks in many important applications.

[10] We can prevent vampire attacks by finding optimal path in wireless sensor network with consideration of load and delay at every node.

III.PROPOSED WORK

Detecting Vampires in Your Network to detect vampires in your network, you need to create an ad-hoc network. A vampire detection system can be installed on a node as an administrative tool. The retrieval requires the IP addresses of all nodes in the network... All incoming packets are monitored. Packet goes through anomaly detection system. IP header analysis includes all fields such as IP header length (IHL), type of service (ToS), identification (ID) and flags. An IP packet header consists of 20 bytes of data, and if the length is less than 20 bytes, the packet is considered anomalous and analyzed before being reported to the administrator. Within the header there is an option to add more optional bytes, but this is not commonly used. The next step in this process is to analyze the TCP or UDP header. The TCP header is based on the unreliable and connectionless IP header. The TCP header occupies 20 bytes and there are some limits on header length. As mentioned above, a normal TCP header is 20 bytes, but TCP can optionally have an additional 40 bytes. So the header size is limited to 60 bytes. There are six TCP flag bits: URG, ACK, PSH, RST, SYN, and FIN, each with a specific use in connection establishment, termination, or control. Only some combinations of the 6 TCP flags can be carried in a TCP packet. The URG and PSH flags can only be used when the packet contains data, such as when the combination of SYN and PSH is invalid. A TCP SYN flood attack floods the network with SYN packets, so each packet is checked for a three-way handshake application. At this stage, the packages fall into two groups: infected packages and normal packages. If the package is infected, the system identifies the package and re-analyzes it to see if it really came from the attacker. Otherwise, normal packets traverse the network and send the data to their destination. Similar to TCP header checking, header checking should be performed on the application layer protocol used in the packet. Packet Filtering Many factors are considered in performing packet filtering. There are three main drivers for this document. Traffic filters each packet according to each protocol, such as TCP, UDP, and ICMP. Group the TCP flags SYN, ACK, RST, FIN and check if the three-way handshake is complete.IP address is valid and not bogus. These elements are important for detection methods to identify which packets are infected packets and distinguish between normal and abnormal packets. Analysis is then performed on each packet using these factors

IV. ALGORITHM

```
Algorithm 1 Forward_packet(p):
        S ←extract_source_address(p)
        C ← closest_next_node(s)
        if (is_neighbour(c)) then
            forward(p,c)
        else
            r ← next_hop_ to_
  non_neighbour (c)
            forward(p,r)
        end if
```

```
Algorithm 2 Secure_ Forward_packet(p):
        s←extract_source_address(p)
        a←exreact_attestation(p)
        if(not verif_source+sig(p)) or
(empty(a) and not is_neighbour(s))
        or )not saowf_verify(a)) then
         return
        for all note in a do
        prevnode ←node
        if(not are_neighbour(node,prenode))
or (not making_progress (prevnode,node))
        then
                return
             end if
          end for
        end if
        c← closest_next_node(s)
        p←saow f_append(p)
        if(is_neighbour(c))then
        forward(P,c)
        else
  forward(P,next_hop_to_non_neighbour(c))
        end if
```

```
Algorithm 3 Modified_ discovery_phase
 (node)
       if (transmit_power(node) >
THRESHOLD) then
          return/*drop(node)*/
     else
          insert_into_routingtable(node)
     end if
```

```
Algorithm 4 Modified_ Forward_packet(p):
        s←extract_source_address(p)
        a←exreact_attestation(p)
        if(not verif_source+sig(p)) or
(empty(a) and not is_neighbour(s))
        or )not saowf_verify(a)) then
        return
        for all note in a do
        prevnode ←node
        if(not are_neighbour(node,prenode))
or (not making_progress (prevnode,node))
        then
               return
           end if
         end for
        end if
        c← closest_next_node(s)
        p←saow f_append(p)
        if(is_neighbour(c))then
        forward(P,c)
        else
forward(P,next_hop_to_non_neighbour(c))
       end if
```

V. OBJECTIVE

The aim of this project is to develop a vampire attack detection system for ad-hoc wireless sensor networks (WSNs) that can identify and mitigate the threat of energy depletion attacks caused by malicious nodes in the network. This paper uses PLGP algorithm in which Vampire attack is detected Carousel Attack and Strech Attack using log file as each node maintains a log file which contains the source, destination and packet id. When the packet will arrive, each node will check the log file and compare the packet id for the source-destination pair of packets. Thus energy consumption for this checking is less compared to the energy drained using infinite looping.

VI. REFERENCES

[1]. Chris Karloff and David Wager "Secure Routing in Wireless Sensor Networks: Attacks and countermeasures" Proc. IEEE Int"l workshop sensor network protocols and applications, 2003

[2]. H. Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003

[3]. M. Tubaishat and S. Madria, "Sensor Networks: An Overview," IEEE Potentials, Vol. 22, No. 2, 2003, pp. 20-23. doi:10.1109/MP.2003.1197877

[4]. J. Deng, R. Han, and S. Mishra, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol 12. 4, pp. 609-619, Aug. 2004

[5]. B. Przydatek, D. Song, and A. Perrig. SIA:Secure information aggregation in sensor network. In ACM SenSys, Nov 2003.

[6]. Cauvery Raju, Defending Against Resource Depletion Attacks in Wireless Sensor Networks

[7]. Anand M, Detection of Vampire Attacks in Ad-Hoc Wireless Sensor Network Evaluation Protection"

[8]. Eugene Y. Vasserman∗and Nicholas Hopper, Vampire attacks:Draining life from wireless ad-hoc sensor networks published on feb 2013(pages 318-332).

[9]. Harpreet Kaur1, Jasmeet Singh Gurm2, Time Based Detection and Prevention of Vampire Attacks in Wireless Sensor Network.

[10]. Aaliya Ali, Prof. Chandu Vaidya ,"A mode switched based routing protocol for multiple sink in wireless sensor network", IJCESR, ISSN (PRINT): 2393-8374, (ONLINE): 2394-0697, VOLUME-5, ISSUE-2, 2018.

Cite this article as :

Gaurav Kawde, Safal Prabhukhanolkar, Shrinivas Tonpewar, Kushagra Belorkar, Shyam Kumar Patle, Chandu Vaidya, "Detection of Vampire Attacks in Ad-Hoc Wireless Sensor Network using PLGP protocol", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 9, Issue 1, pp.195-199, January-February-2023. Available at doi :
https://doi.org/10.32628/CSEIT2390135
Journal URL : https://ijsrcseit.com/CSEIT2390135