INTERNATIONAL JOURNAL OF PURE AND APPLIED RESEARCH IN ENGINEERING AND TECHNOLOGY

A PATH FOR HORIZING YOUR INNOVATIVE WORK

ROUTING PROTOCOL ATTACK IN WIRELESS SENSOR NETWORK

MRS. PRITI LALE[1], DR. G.R. BAMNOTE[2]

1. M.E (CSE-Pursuing), PRMIT & R, Bandera, Amravati.
2. Head, Computer Engg. Department, PRMIT & R, Bandera, Amravati.

Accepted Date: 15/02/2014 ; Published Date: 01/04/2014

Abstract: Ad-hoc networks serves the purpose of connecting nodes instantly, without infrastructure. Threats posed by Denial of Service (DoS) attacks against 802.11's MAC protocol. Such attacks, which prevent legitimate users from accessing the network, are a vexing problem in all networks, but they are particularly threatening in the wireless context. Resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes is very difficult to detect. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. This paper specifies different routing protocol attack and tries to detect one of such attack by using simulation result and bound the damage of such attack.

Keywords: Denial of services, Vampire attack, Wireless sensor network.

Corresponding Author: MRS. PRITI LALE

Access Online On:

www.ijpret.com

How to Cite This Article:

Priti Lale, IJPRET, 2014; Volume 2 (8): 9-16

PAPER-QR CODE

INTRODUCTION

Ad hoc wireless sensor network is very interesting target because it offers a large attack surface and interesting playground for creative attack ideas. The main possibilities to attack WSNs include all the classical techniques known from classical system security. The ability of an attacker to access the internal state of a sensor node seems particularly characteristics for sensor network. This type of attack is called node capture. Depending on the WSN architecture, node capture attacks can have significant impact. Thus, most existing routing schemes for WSNs can be substantially influenced even through capture of a minute portion of the network. In this paper some ad hoc wireless sensor network attacks has been discuss and one of such attack is detected.

As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. Due to their ad-hoc organization, wireless ad-hoc networks are particularly vulnerable to denial of service (DoS) attacks, and a great deal of research has been done to enhance survivability.

I. Literature Survey

The recent attack on popular web sites like yahoo, eBay and E*Trade and their consequent disruption of services have exposed the vulnerability of the internet to DDos attacks. The TCP SYN flooding is the most commonly used attack. It consists of a stream of spoofed TCP SYN packet directed to a listening TCP port of the victim. The SYN flooding attacks exploit the TCPs three way hand shake mechanism and its limitation in maintaining half open connection[4][6]. To counter SYN flooding attacks several defense mechanism such as Syn cache , Syn cookies, SynDefender, Sun proxing and Synkill.has been use[4].

In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them (possibly selectively) to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems [9]. If the attacker performs this tunneling honestly and reliably, no harm is done; the attacker actually provides a useful service in connecting the network more efficiently. However, the wormhole puts the attacker in a very powerful position relative to other nodes in the network, and the attacker could exploit this position in a variety of ways[1][3].

In Carousel attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route [4].

Reduction of quality of attacks is a new category of attacks that target the adaptation mechanism of the current internet system [7]. DoS and wormhole attacks are exponentially increasing in frequency, complexity, and scope of damage attacks, which prevent legitimate users from accessing the network, are a vexing problem in all networks, but they are particularly threatening in the wireless context[8]. Without a physical infrastructure, an attacker is afforded considerable flexibility in deciding where and when to attack, as well as enhanced anonymity due to the difficulty in locating the source of individual wireless transmissions [2]. Moreover, the relative immaturity of 802.11-based network management tools makes it unlikely that a well-planned attack will be quickly diagnosed[6].

In this paper Vampire attack which is wireless ad-hoc sensor network attack is detected and prevented. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance-vector, source routing and geographic and beacon routing [6]. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol compliant messages, these attacks are very difficult to detect and prevent.

Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol compliant messages [5]. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behavior and cannot optimize out malicious action.

II. Comparison with other attacks

A attack which is earliest detected and prevented attack is DDoS attack . It is an attempt to make a machine or network resource unavailable to its intended users by saturating the target machine with external communication requests. Sleep deprivation attacks are similar kind of attack in which three main forms of attack are their which is service request power attacks ,benign power attacks, malignant power attacks. In first attack the valid network service request such as telnet, ssh and web server request keeps the device busy authenticating or servicing the request .In second attack device is made to execute a valid but energy-hungry task indefinitely which drain the energy source. The third attack maliciously penetrates the system and alters operating system kernel such that more energy needed to execute them.

The vampire attack is rather different from the earlier discuss attack because it is a very basic attack which will not make any special effort to drain energy of nodes but use the vulnerabilities of routing protocol that's why the detection is difficult. In this system it has been shown by using no. of nodes and traversing them through different nodes detection has been done after detection the malicious data had been deleted and it will make the packet empty which have malicious data. So the energy from the remaining node will not drain and the node works properly using its full efficiency that's the way improvement in throughput has been done.

III.System Architecture & Results

System Architecture

In this system we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

As vampire attack do not rely on the design properties of any routing protocol but uses the vulnerabilities of protocol this simulation results shows detection and prevention.

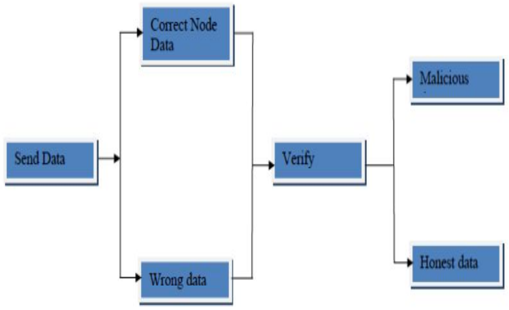
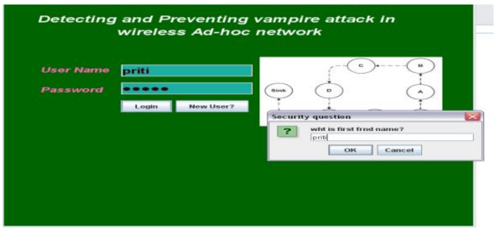


Fig.1 System Architecture

Results

In this system detection of vampire attack has been done by using simulation results. For detection of vampire attack we present simulation result in which number of nodes are considered through which data goes from one node to another. For authentication purpose login has been specified which is one part of identifying the user is honest or malicious. Following figure shows these results.


Detecting and Preventing vampire attack in wireless Ad-hoc network

User Name: priti

Password: ●●●●●

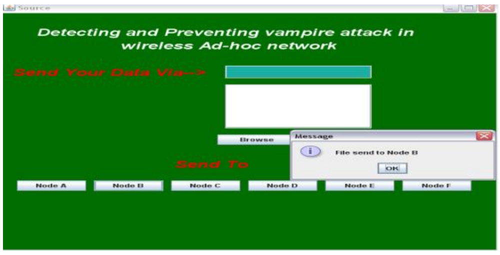
Security question

wht is first frnd name?

priti

Fig.2 User Authentication

In Fig.2 user authentication has been done in which security question is one part of authentication.


Detecting and Preventing vampire attack in wireless Ad-hoc network

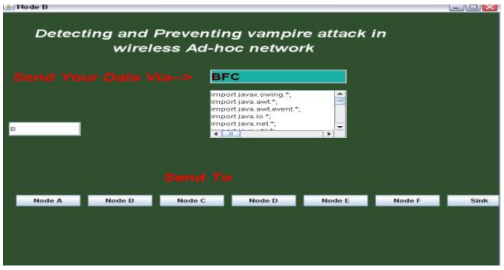
Send Your Data Via-->

Message

File send to Node B

Fig.3 Node A, B, C, D, E & F

In Simulation result 6 nodes has been considered for forwarding node from one to another shown in Fig.3


Detecting and Preventing vampire attack in wireless Ad-hoc network

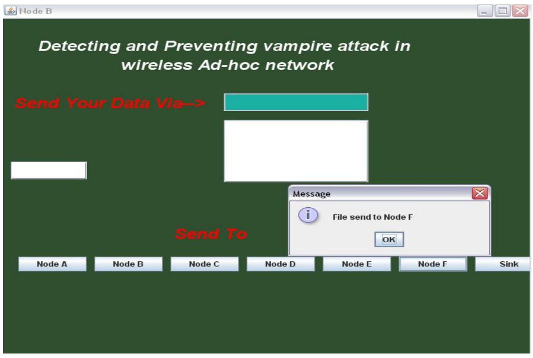
Send Your Data Via--> BFC

```
import javax.swing.*;
import java.awt.*;
import java.awt.event.*;
import java.io.*;
import java.net.*;
```

B

Fig.4 Node B to Node F

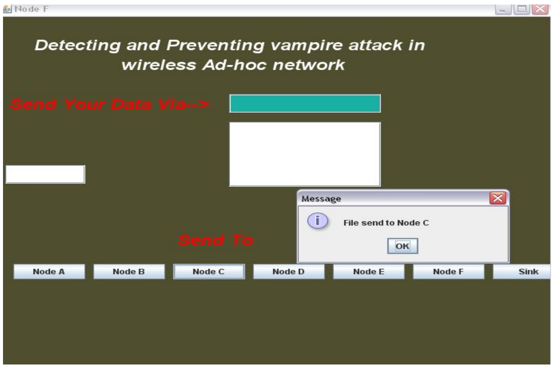
In Fig.4 data forwarded from Node B to Node F.


Detecting and Preventing vampire attack in wireless Ad-hoc network

Message: File send to Node F

Fig.5 Node F to C

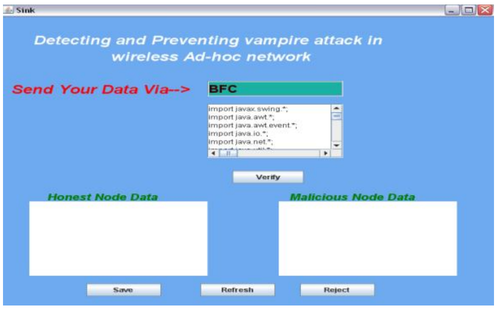
In Fig.5 data forwarded from Node F to Node C.


Detecting and Preventing vampire attack in wireless Ad-hoc network

Message: File send to Node C

Fig.6 Node C to Sink

For detecting the vampire attack the data has been forwarded to sink which has been shown in Fig.6

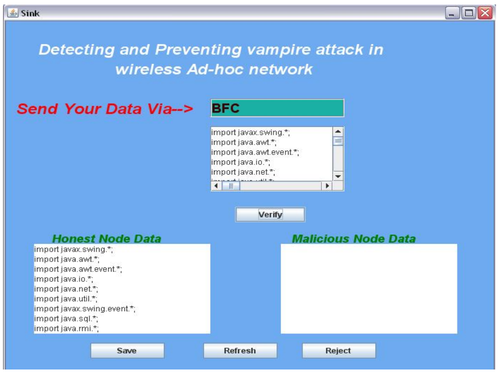

Detecting and Preventing vampire attack in wireless Ad-hoc network

Send Your Data Via--> BFC

```
import javax.swing.*;
import java.awt.*;
import java.awt.event.*;
import java.io.*;
import java.net.*;
```

Fig.7 Verification

For detection the vampire attack the data has been verified which has been shown in Fig.7



```
import javax.swing.*;
import java.awt.*;
import java.awt.event.*;
import java.io.*;
import java.net.*;
```

```
import javax.swing.*;
import java.awt.*;
import java.awt.event.*;
import java.io.*;
import java.net.*;
import java.util.*;
import javax.swing.event.*;
import java.sql.*;
import java.rmi.*;
```

Fig.8 Detecting Honest Node Data

In Fig.8 The verification result has been shown in which the traverse data is honest node data

In the above figures vampire attack has been detected, if the user is a valid user the path specified is traversing through three nodes. when the user is a malicious one who is trying to forward malicious data the path excedded upto six node in which the malicious data drain the energy of all the nodes in the network making the node lifeless.

IV.Conclusion

The Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes' battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. The proposed system showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly-generated topology of nodes.

V. References

1. Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.
2. David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, Effects of denial-of-sleep attacks on wireless sensor network MAC protocols, IEEE Transactions on Vehicular Technology 58 (2009), no. 1.

3. Frank Stajano and Ross Anderson, The resurrecting duckling: security issues for ad-hoc wireless networks, International workshop on security protocols, 1999.
4. Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.
5. Ivan Stojmenovic and Xu Lin Power Aware Localized routing in Wireless network ,IEEE Transaction on Parallel and Distributed System Vol.12 No.10 October 2001.
6. John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.
7. Jing Deng, Richard Han, and Shivakant Mishra, Defending against pathbased DoS attacks in wireless sensor networks, ACM workshop on security of ad hoc and sensor networks, 2005.
8. Rahul C. Shah and Jan M. Rabaey, Energy aware routing for low energy ad hoc sensor networks.
9. Wormhole Attacks in Wireless Networks Yih-Chun Hu, *Member, IEEE,* Adrian Perrig, *Member, IEEE,* and David B. Johnson, *Member, IEEE.*