www.ierjournal.org International Engineering Research Journal (IERJ) Volume 1 ZCOER Issue Page 1-4,
2017, ISSN 2395-1621

DETECTION AND AVOIDANCE OF VAMPIRE ATTACK IN WIRELESS SENSOR NETWORK

[#1]Sukhada S Kadam, [#2]Aboli N Jori,
[#3]Ashlesha S Pachore, [#4]Harshal R Sarade.
Comp Dept, Savitribai Phule Pune University,
Pune-41, Maharashtra.,India

[1]*kadamsukhada7@gmail.com* , [2]*joriaboli@gmail.com* , [3]ashleshapachore@gmail.com , [4] harshalsarade4@gmail.com

[#1234] Zeal College of Engineering, Pune, Maharashtra, India

ABSTRACT

Ad hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Security work is prioritized in this area and focusing primarily at medium access control or the routing levels on denial of communication. This vampire attack impacts by persistently disabling the network and causing the nodes battery power drain drastically.
Vampire attacks can be easily executed using even a single malicious intruder, who sends simply protocol complaint message, these vampire attacks are thus destructing and very hard to detect. A new proof-of-concept protocol is a method to mitigate these kinds of attacks. This protocol limits the damage caused at the time of packet forwarding.

ARTICLE INFO

Article History
Received: th 2017
Received in revised form :
th 2017
Accepted:th 2017
Published online :
th 2017

Keywords— pervasive computing, security, vampire attack, denial, protocol.

I. INTRODUCTION

Wireless Sensor Network (WSN) comprises sensor nodes which communicate wirelessly and to carry out some specific function, it forms ad-hoc networks. In nearby time to come, ad-hoc wireless sensor networks (WSNs) will come with the latest applications, like on-demand computing power, unbroken connectivity and immediately-operational communication for military and also for the initial responders. These networks check physical or environmental circumstances like sound, temperature, pressure, etc. to transfer the information to a key location via network. Availability faults become less tolerable. This lack of availability makes the difference between industry and power outages, lost productivity, environmental destruction and also lost lives.

Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attack at the routing protocol layer, which permanently disable networks by quickly draining nodes battery power. These Vampire attacks are not specific protocol, but rather rely on the properties of many popular classes of routing protocols. This paper also considers the down fall of the routing protocols leading to lack in safety from vampire attacks as the node's energy is drained in the networks. Dos, reduction of quality (RoQ) and routing infrastructure attacks, these attacks vary, as they work intentionally to disrupt the network completely, but they don't disrupt immediate availability. Vampire attacks are independent of overflowing the network with huge volumes of data in fact they attempt to pass on small amount of data as much as possible to attain the highest energy depletion avoiding a rate limiting outcome. These attacks are tough to discover and mitigate. We find that all examined protocols are susceptible to vampire attacks, which are devastating, difficult to detect and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages.

In the worst case, a single Vampire can increase network wide energy usage by a factor of ON, where N in

the number of network nodes. Methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

II. MOTIVATION OF THE PROJECT

At first glance, energy vampires can seem highly attractive. They often are good-looking, bold, intelligent, and may appear to have a high opinion of you as indicated by their flattering attention. Drawing you into their inner circle may seem like just the boost you need in your usually drab work environment.

III. PROBLEM STATEMENT

Detection and Avoidance of Vampire attack in Wireless Sensor Networks. 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, and source routing and geographic and become routing.
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 these vampire attacks use protocol-compliant messages, these vampire attacks are very difficult to detect and prev

IV. GOALS AND OBJECTIVES

- To detect the attack accurately without accusing a legitimate node as attacker.
- Proposed Protocols should achieve the security under hostile and suspicious scenarios.
- Energy Efficient path Detection.
- To maximize the lifetime of network.
- To increases the lifetime of the sensor nodes.
- To study previous routing protocols and their features.
- Develop a simulated environment of WSN having configurable parameter.

V. EXISTING SYSTEM

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. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behavior and cannot optimize out malicious action.

Disadvantages Of Existing System:

- Power outages
- Due to Environmental disasters, loss in the information
- Lost productivity
- Various DOS attacks
- Secure level is low
- They do not address attacks that affect long-term availability.

VI. PROPOSED SYSTEM

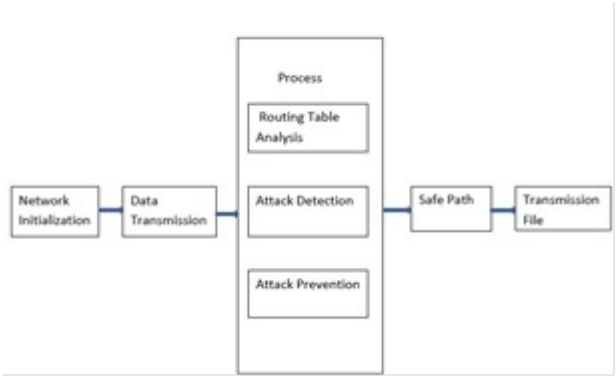

Fig.3: Proposed System

This work makes four primary contributions .First, data is transferred through normal communication that is source
nodes sends the route request packets and destination responds to them via shortest path. Second, during data transfer if there are routing loops between intermediate nodes then carousel attack has been detected. Third, if the route from source to destination is very long traversing many nodes in the network then the stretch attack has been detected.
Finally, the time taken to transfer the data in normal communication is compared with the time in the occurrence of both carousel and stretch attacks. If the time taken during attacks is more than time of normal communication then new path is chosen, which is free from attacks. In proposed system simulation results are shown quantifying the performance of both carousel attack and stretch attack. Then, existing route is modified to provably bound the damage from Vampire attacks during packet forwarding.

1) Carousel attack

In the carousel attack, attackers introduce some packet within a route tranquil as a sequence of loops, such that the same node appears in the route of communication many times. This attack increases the routing length and delay very much in the networks and also inadequate by the number of allowable entries in the resource route. According to the fig.1 it is clearly seen that source send the data packet which marked as 1to node A. Node A send it to

node B. later on data packet transmitted to other nodes in the network. But instead of transmitting the data to source from node E it transmits to node F and again transmits to node A. This is done due to the corruptness nature of the data packet which is transmitting by compromised source. Thus heavy wastage of energy occurs.

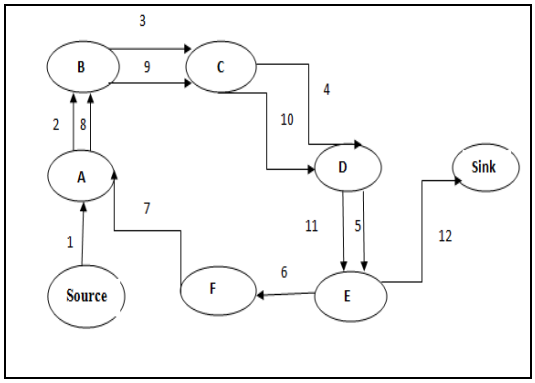

Fig.1: Carousel Attack

Algorithm for Carousel Attack

1. Set unique id for each node in the network.
2. Source node forward a packet add id of source to a string.
3. As next node gets the packet it appends its own id and checks if the id for repeatation..
4. If (id is repeated)

   Carousel attack

   Else

   Node appends its own id & forwards it to next.
5. **Pseudo code :**

```
Begin

Initialization

For(int i=0;i<network node;i++)
{

Node[0]=i;

}

NodeArray[] = nodeString.toCharArray();

For( i=0;i<NodeArray.length;i++)

{

For(int j=i+1;j<NodeArray.length;j++)

{

If(NodeArray[i]==NodeArray[j])

{

Carousel Attack Detected

}

}

}

Packet = nodeString  + id;

Forward (NextNode);

End
```

2) Stretch attack

In stretch attack a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. A sincere source will choose the path, Source-> F ->E -> Sink, which affects four nodes including itself, but the nasty node choose a lengthy path which affects all nodes in the network is shown in Fig. 2.

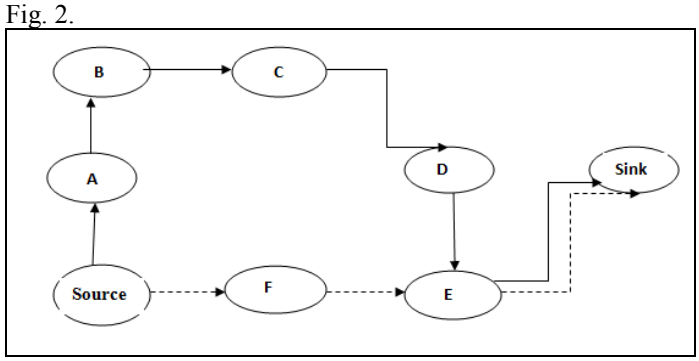

Fig. 2 : Stretch Attack

These paths cause nodes that do not lie along the sincere path to consume energy by transmitting packets they will not receive in honest scenarios. An attacker forms lengthy paths, which passes through every node in the network and also increases length of packets that causes packets to be processed by a number of nodes.

Algorithm for Stretch Attack

1. The ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant.
2. An adversary constructs artificially long routes, potentially traversing every node in the network.
3. Increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination.

4. Pseudo code :

```
Begin

StretchAttack(ipaddress)

{

  Extract the closest neighbour

 If(neighbour!=listed)

 {

 if (neighbour!=receiver)

 {

    Forward packet.

}
Else

{
StretchAttack(ipaddres,packet)
}
}
}

End
```

VII. ENCRYPTION FUCTION

Encryption is the most effective way to achieve data security. To read an encrypted file, you must have access to a secret key or password that enables you to decrypt it. Unencrypted data is called plain text and encrypted data is referred to as cipher text.
The primary purpose of encryption is to protect the confidentiality of digital data stored on computer systems or transmitted via the Internet or other computer networks. Modern encryption algorithms play a vital role in the security assurance of IT systems and communications as they can provide not only confidentiality, but also the following key elements of security:

Authentication: the origin of a message can be verified.
Integrity: proof that the contents of a message have not been changed since it was sent.
Non-repudiation: the sender of a message cannot deny sending the message.

VIII. DECRYPTION FUNCTION

Decryption is the process of taking encrypted text and converting it back into text that you or the computer can read and understand. This term could be used to describe a method of un-encrypting the data manually or with un-encrypting the data using the proper codes or keys.
One of the foremost reasons for implementing an encryption-decryption system is privacy. As information travels over the World Wide Web, it becomes subject to scrutiny and access from unauthorized organizations. As a result, data is encrypted to reduce data loss and theft. Some of the common items that are encrypted include email messages, text files, images, user data and directories. The person in charge of decryption receives a prompt or window in which a password may be entered to access encrypted information.

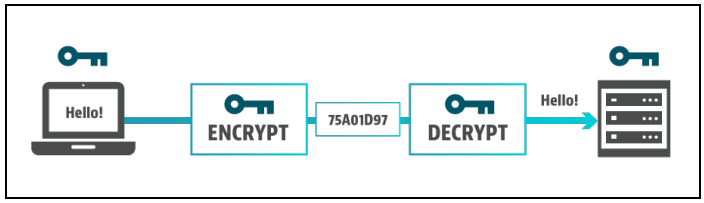

Fig. 4 : Encryption and Decryption Function

IX. MATHEMATICAL MODEL

System Description:

- Sc=[S, E, input, output , success ,failure]
- S=Start State
- E=End State
- Input:
  Select Source node and Destination node.
- Output:
  Blocked node, Energy efficient path, energy deficient path, attack type attack name, attack avoidance strategy
- Success Conditions: Successfully detect attack.
- Failure Conditions: Fails to detect extended path.

X. CONCLUSION

Vampire attack deactivates ad-hoc wireless sensor network by reducing battery life of nodes. The attack does not rely on specific protocols. Actually it depicts vulnerabilities in various well-known protocol classes. Proposed protocol prevents from transmit-ting phase attacks and ensure that packets constantly make progress in direction of their destination Vampire attacks has been defined as a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes battery power. The sensor network routing protocol that reduces the dam-age from Vampire attacks by verifying that packets consistently make progress toward their destinations. The

routing protocol has been used at the time of routing to make efficient energy utilization during the packet forwarding phase.

XI. REFRENCES

[1] A.Anto Jenifer, V.Thangam and N.Jeenath Laila, "Maintaining Lifetime of Wireless Adhoc Sensor Networks by Mitigating Vampire Attacks", IJIRST International Journal for Innovative Research in Science and Technology, Volume 1, Issue 9, February 2015.

[2] Eugene Y. Meghana N and Dr. G. F. Ali Ahammed, "A Survey on Vampire Attacks in Wireless Ad-Hoc Sensor Networks", International Journal of Advanced Research in Computer Science and Software Engineering,Volume 5, Issue 5, May 2015.

[3] Dantam.Ramesh, Dasari .Koteswara Rao,"Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor communication of Networks", International Journal of Research in Computer and Communication Technology, Vol 3, Issue 9, September - 2014.

[4] K.Vanitha, V.Dhivya, "A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Network", IJIRSET Volume 3, Special Issue 3, March 2014.

[5] P.PreethiMonolin, Dr.J. Amutharaj" Cache Consistency and IDS for Handling Attacks in Routing Ad-hoc networks"April 2014.

[6] Lina R. Deshmukh and Amol D. Potgantwar "Prevention of Vampire Attacks in WSN Using Routing Loop", proc. IRF International Conference, February 2014.

[7] Priti Lale and Dr. G.R. Bamnote "Detecting and preventing vampire attack in wireless sensor network" proc. Scientific & Engineering Research International conference, Volume 4, Issue 12, December 2013.

[8] "The Network Simulator – ns 2, http://www.isi.edu /nsnam/ns, 2012.

[9] Gowrishankar.S, T.G.Basavaraju, Manjaiah D.H, Subir Kumar Sarkar "Issues in Wireless Sensor Networks" July 2 - 4, 2008, London, U.K.

[10] GergelyAcs, LeventeButtyan, and IstvanVajda, Provably secure ondemand source routing in mobile ad hoc networks, IEEE Transactions on Mobile Computing 05 (2006), no. 11.

[11] Shyamala Ramachandran and Valli Shanmugam "Detecting and preventing vampire attack in wireless sensor network" proc. Sensor & Ubiquitous Computing International journal of ad-hoc, Vol.3, No.4, August 2012.

[12] B. Umakanth and J. Damodhar "Detection of Energy draining attack using EWMA in Wireless Ad Hoc Sensor Networks"proc. IJETT, vol. 4, Issue 8, 2013.

[13] T.Sathyamorthi, D.Vijayachakaravarthy, R.Divya, M.Nandhini "A Simple and Effective Scheme to find Malicious node in Wireless Sensor Network" International Journal of Research in Engg. And Tech.,Vol. 3, Issue 2, 2014.

[14] Thanmanam. P and Suguna. M "Detection of Vampire Attacks using Optimal Energy Boost-up Protocol in WSN's" IJETCSE, Vol. 8,issue 1, 2014.

[15] K. Sivakumar and P.Murugapriya "Efficient Detection and Elimination of Vampire Attacks in Wireless Ad-Hoc Sensor Networks" proc. International Conference On Global Innovations In Computing Technology, Vol. 2, Issue 1, 2014.