ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

Vol. 3, Issue 7, July 2015

Vampire Attack: Solution using Energy Efficient Trust Value

Pritam M. Channawar, Y. V. Chavan

Dept. of Computer Engineering, PVPIT, Pune, Maharashtra, India

ABSTRACT Ad hoc low power wireless networks are existing research for sensing and common computing. This paper defines resource depletion attach which forms at routing protocol layer. This attack disables the entire network by consuming nodes battery power. These attacks are not dependent on any protocol but depend on many class of routing protocols. We discussed all protocols are susceptible to Vampire attacks, which are dangerous, difficult to detect, and are very easy to carry out using very few such as one malicious insider sending only protocol-compliant messages. Proposed algorithm gives the solution for carousal attack and stretch attack to achieve better security over these attacks. Also introduce trust based energy efficient technique to keep network active in vampire attack. This technique also helps to detect and avoid malicious nodes in the routing phase.

KEYWORDS: wireless networks; ad hoc network; attack; routing protocol; security

I. Introduction

Ad hoc wireless sensor networks are becoming more popular and demanding techniques in near future they provides applications such as on demand computing and also it gives continuous connectivity, quick communications. This type of network provides availability, it monitors environmental conditions, but in every day functioning WSN becomes very critical to handle and also the availability is becoming crucial issue. People cannot use it efficiently because availability faults are less acceptable. Unavailability can affect the consistency and productivity of an organization, so that high availability is required for better performance of the organization. Because the structure of organization is ad hoc it will resist denial of service attack. Availability is important factor to improve the performance of organization so that user can use network without any complexity.

This paper introduces scheme that gives solution to short term availability attacks of network but do not work long term availability attacks. The denial of service attack is very important attack that cannot be neglected because it depletes nodes battery power by consuming all its energy. Dos attack is kind of resource depletion attack in this resource of interest is nodes battery power. In this we study the routing protocols which are designed to protect from attack and provide security are less protective from these attacks, this attack is called as vampire attack. The vampire attack are not dependent on protocol they are independent of design properties and implementation fault of specific routing protocol [1].

II. Related work

Dos attack, Quality of service attack and battery depletion attacks come in previous studies. Early mention of this power exhaustion was found as sleep depletion torture [7]. Given attack prevents node from starting low power sleepy cycle and so consumes their batteries very fast [2].

In this paper we present damages caused by vampire attack and the protection from various protocol also we study hoe to recover from them. In this we study how source node give long path to reach the destination so that the battery power of anode is consumed very fast and node get depleted. In the concept of routing decision of forwarding depends on the node independently [1]. In this we propose directional antenna and warm whole attack which are used to send the packets to multiple remote locations, also it will increase energy cost in the whole network [3]. We keep track of both forwarding phase and topology discovery phase because if the messages in discovery are overloaded then it requires energy at each node [2]. In attack called carousel attack the attacker purposely shows routing loops and

DOI: 10.15680/ijircce.2015. 0307006

consumes nodes battery power. Another attack called stretch attack in this the attacker shows longer route than the shorter route to deplete the nodes battery power [3].

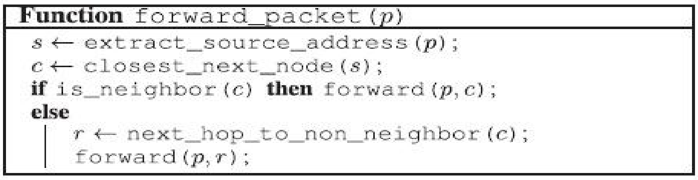
III. Attack on Stateful Protocol

In stateless protocols the nodes are aware of topology of network and state of the topology. Depending on this state the nodes make decisions about forwarding. Here are two main types of stateful protocols that are link state and distance vector routing. First we will see the link state routing in which nodes keeps track on state of the link that is it checks that whether the link is up or down. Another is distance vector routing which keeps track of which is the next node.

IV. Existing Method

In PLGP to get security from vampire attack routing protocol can be modified through packet forwarding phase. There are two phases in PLGP that are topology discovery phase and packet forwarding phase. The original version of this protocol in not secure for vampire attacks.

In PLGP to get security from vampire attack routing protocol can be modified through packet forwarding phase. There are two phases in PLGP that are topology discovery phase and packet forwarding phase. The original version of this protocol in not secure for vampire attacks.



```
Function forward_packet(p)
    s ← extract_source_address(p);
    c ← closest_next_node(s);
    if is_neighbor(c) then forward(p, c);
    else
        r ← next_hop_to_non_neighbor(c);
        forward(p, r);
```

V. Security over Vampire Attack

To get security against vampire attack we make some changes in forwarding phase of PLGP to ignore the vampire attack. In this we first study the no-backtracking property. No-backtracking is satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. Formally

Definition: No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network [1].

A. *Problem Statement*

Existing system do not provide satisfactory solution for given Vampire attacks through the topology discovery phase. It introduces some new information about damage limitations and possible with further modification to PLGPa. Pure solution to these problems is given in proposed system. Also it provide solution to handle mobile network.

B. *Objectives*

- Forward same packet repeatedly
- Dropping packets
- Battery consumption
- Deviation from proper path

C. *Proposed System*

We introduce new class of solution to get solution for above issues

- Proposed system keeps track of forwarded packet to avoid duplication of packet.
- Proposed system tries to neglect malicious nodes using the packet to energy ratio, so that extra energy will not be consumed.
- An alternate path is considered when node drops packet.

D. *Solution Outline*

- Generate technique to avoid carousel attack.
- Generate technique to avoid stretch attack.

ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

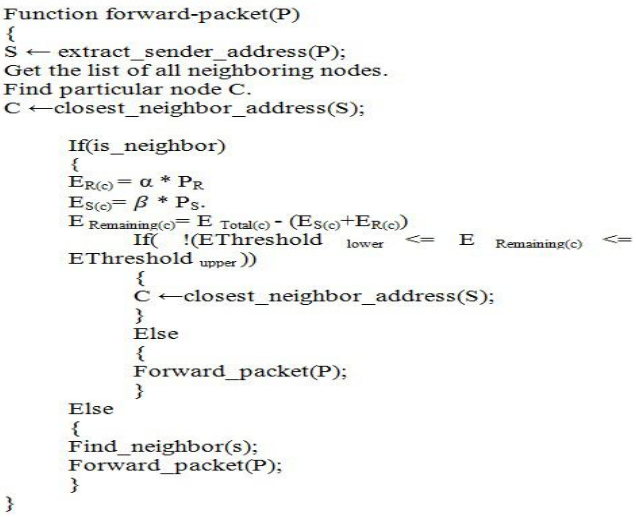
Vol. 3, Issue 7, July 2015

- Generate factor of trust.

VI. PROPOSED METHOD

A. *Prevention From Carousel Attack And Stretch Attack*

This paper has introduced carousel attack and its harmful effect on network. New design or technique is required to protect from this violation. In a WSN network when packet of message is sent from sender to receiver, these messages are forwarded by intermediate nodes present in the network and this process continues flow till it reaches to the receiver. In this prevention technique the carousel attack is controlled by operating various verifications that will confirm that the packets will not go into infinite loop by consuming node battery power. For this validation we perform two functional operation forward-packets(p) and verify-packets(p) here p is packet. First we will see the steps involved in packet forwarding. The algorithm shown gives idea about this concept.



```
Function forward-packet(P)
{
S ← extract_sender_address(P);
Get the list of all neighboring nodes.
Find particular node C.
C ←closest_neighbor_address(S);

    If(is_neighbor)
    {
    $E_{R(c)} = \alpha * P_R$
    $E_{S(c)} = \beta * P_S$.
    $E_{Remaining(c)} = E_{Total(c)} - (E_{S(c)} + E_{R(c)})$
        If( !(EThreshold_lower <= E_Remaining(c) <=
    EThreshold_upper ))
        {
        C ←closest_neighbor_address(S);
        }
        Else
        {
        Forward_packet(P);
        }
    Else
    {
    Find_neighbor(s);
    Forward_packet(P);
    }
}
```

The above algorithm is used for forwarding the packets by intermediate node. The algorithm extracts the information from source address, this includes IP address of source and destination, then node check whether the IP address his own node and with the destination node, if it matches this means the packet was sent to him only and the process terminates. There can be another condition that the IP address of node and destination doesn't matches, in this case it will forward the packet to closest node.

In proposed method the stretch attack can be prevented by using the shortest path method. When the packets are sent from source to destination the shortest path is chosen based on nearest neighbour that reaches to destination from source. To prevent from stretch attack list of all neighbour is calculated in array based on that path is decided. In this way the attack is prevented

B. *Calculation Of Energy Efficiency Trust Value*

Energy efficient trust value of its neighbouring node is calculated by every node of the wireless network. To calculate the trust value of node x and C we use following steps.

1. Get the list of all neighboring nodes.
2. Find particular node C.
3. Calculate the amount of energy consumed by node C for receiving and forwarding packet.
4. $E_{R(c)} = \alpha * P_R$

Here E_R= is the amount of energy consumed by node C to receive all incoming packet.
α= is the configurable parameter (amount of energy required to receive a packet).
P_R= No. of packets received.

5. $E_{S(c)} = \beta * P_S$.

Here E_s= is the amount of energy consumed by node C to send all outgoing packet.
β = is the configurable parameter.(amount of energy required to send a packet to next hop).
P_s= No. of packets sent.

6. $E_{Remaining(c)} = E_{Total(c)} - (E_{S(c)} + E_{R(c)})$
7. $EThreshold_{upper} = EThreshold_{Remaining} + \gamma$.

$EThreshold_{upper}$ = Gives upper bound on threshold.
$EThreshold_{Remaining}$ = Gives average remaining threshold energy of the WSN.
γ = Configurable parameter.

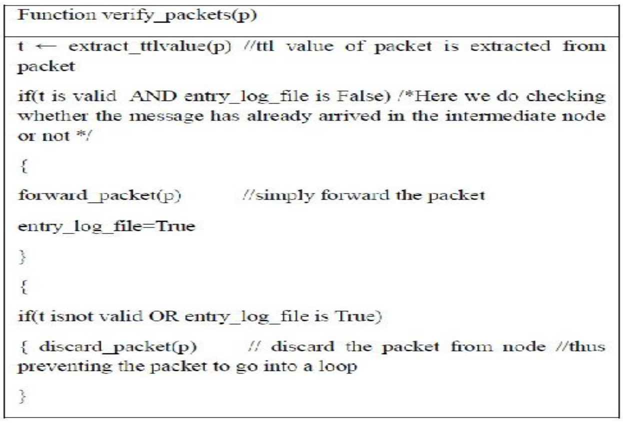
8. $EThreshold_{lower} = EThreshold_{Remaining} - \lambda$.

$EThreshold_{lower}$= Gives lower bound on threshold.
λ = Configurable parameter.

9. $EThreshold_{lower} <= E_{Remaining(c)} <= EThreshold_{upper}$

In last equation if Eremaining is less than the lower bound then that node may discard the packet. Such as, if Eremaining is more than the upper bound then such node is called as malicious.

The verify-packets(p) function will keep track of whether new packet has already entered in the intermediate node or not. So for this purpose we are continuously checking the message for duplication in node. As the same packet detected at node it will cancel the packet and prevent from duplication of packets in the entire network.



```
Function verify_packets(p)
t ← extract_ttlvalue(p)  //ttl value of packet is extracted from packet
if(t is valid  AND entry_log_file is False) /*Here we do checking whether the message has already arrived in the intermediate node or not */
{
forward_packet(p)          //simply forward the packet
entry_log_file=True
}
{
if(t isnot valid OR entry_log_file is True)
{ discard_packet(p)        // discard the packet from node //thus preventing the packet to go into a loop
}
```

VII. SIMULATION RESULT

A. *Result Snapshot*

Figure 1 shows the snapshot of graphical user interface where there are number of input fields such as number of nodes, Source node, Destination node, Simulation time and buttons such as Draw nodes, Attack send, Normal send, Stop, Exit. Figure 2 shows how the nodes are drawn according to the input of a user.

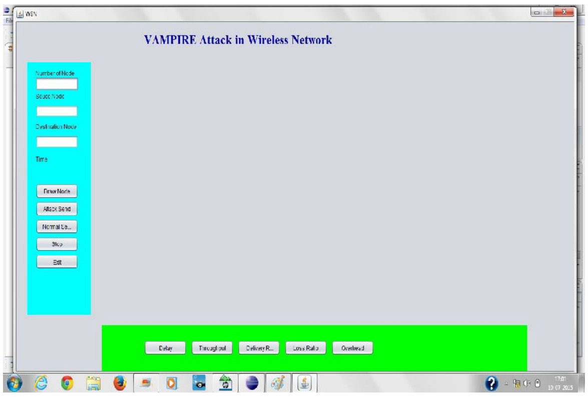
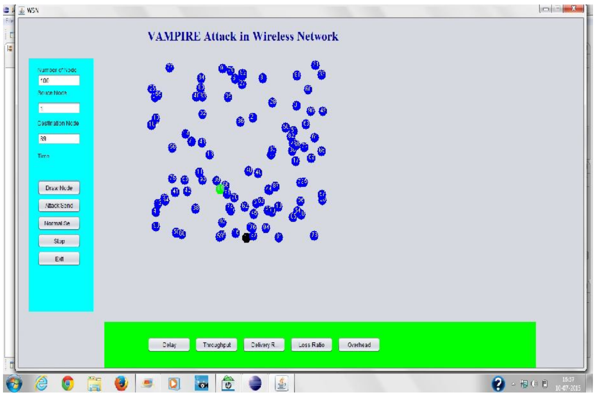


Figure 1: GUI



Number of Node 100
Souce Node 1
Destination Node 39
Time

Figure 2: Nodes in WSN

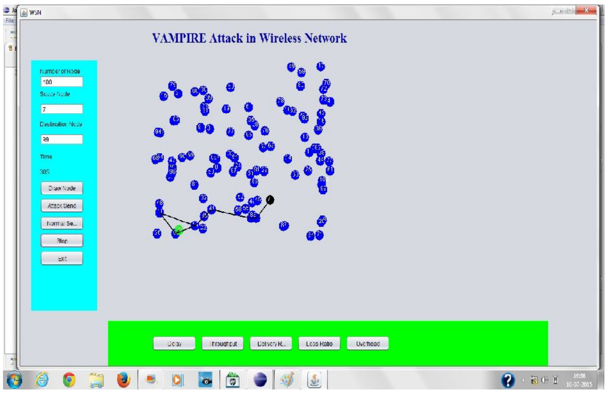
ISSN(Online): 2320-9801
ISSN (Print): 2320-9798

International Journal of Innovative Research in Computer and Communication Engineering

(An ISO 3297: 2007 Certified Organization)

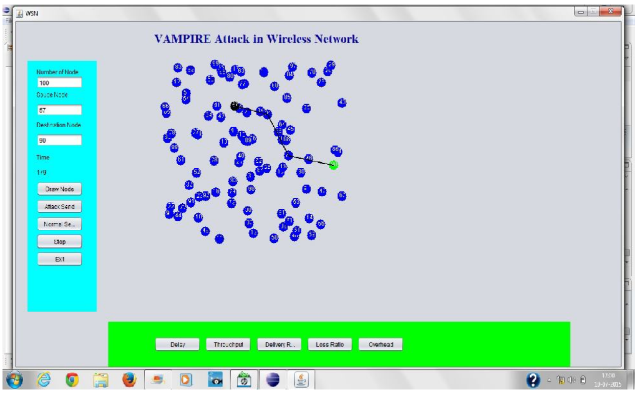
Vol. 3, Issue 7, July 2015

Figure 3 and figure 4 shows the packet sending in vampire attack and honest rout in wireless sensor network. In figure 3 both the stretch and carousel attack are shown where loops are formed and long path is taken to consumes the WSN energy and deplete the battery power. In figure 4 these attacks are removed and shortest path is chosen to save battery depletion and to prevent from attack.


WSN

VAMPIRE Attack in Wireless Network

Number of Node: 100
Souce Node: 7
Destination Node: 99
Time: 305


WSN

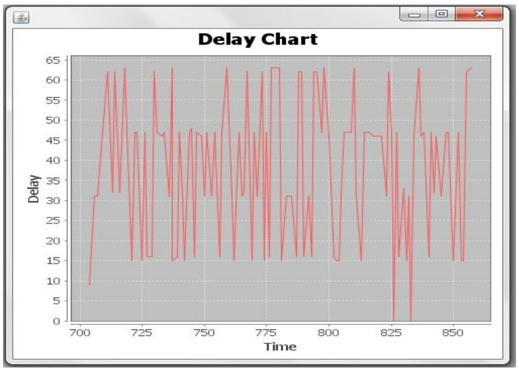
VAMPIRE Attack in Wireless Network

Number of Node: 100
Souce Node: 57
Destination Node: 90
Time: 179

Figure 3 : Vampire attack

Figure 4 : Honest rout

B. *Result Analysis*



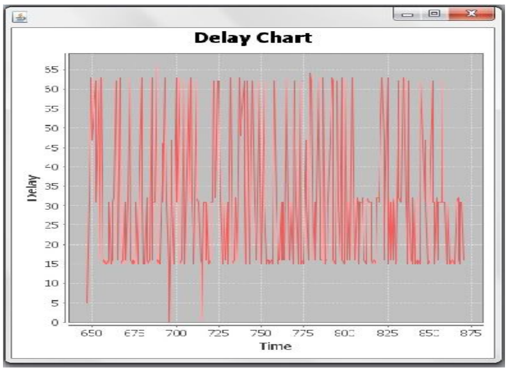


Figure 5(a): Delay in attack

Figure 5(b): Delay in honest rout

A figure 5 show the simulation result of both vampire attack as well as honest rout delay rate varies in both, in attack delay is more as compared to honest rout, so that the efficiency of a network increases.

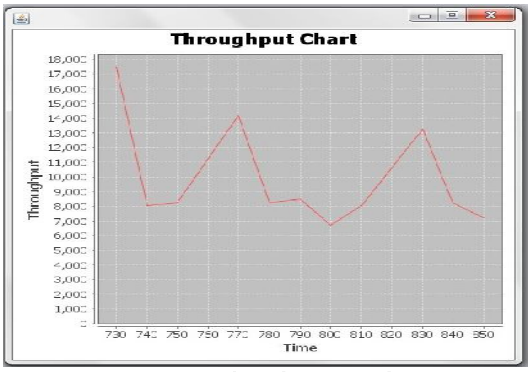


Figure 6(a): Throughput in attack

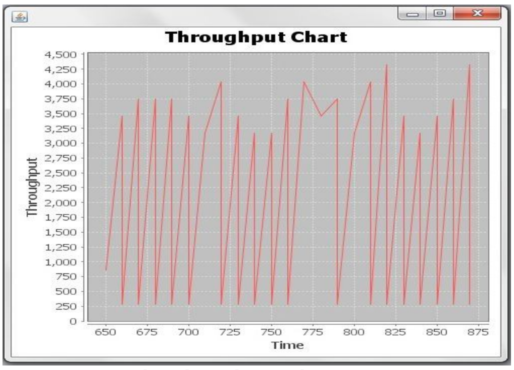


Figure 6(b): Throughput in honest rout

DOI: 10.15680/ijircce.2015. 0307006

Throughput or network throughput is the rate of successful message delivery over a communication channel. As shown in figure 6(a) and (b) throughput decreases in attack and in honest rout the rate increases. These result shows proposed method is working well against attack.

VIII. CONCLUSION

The definition of vampire attack is nothing but a new type of resource consumption attack this attack uses routing protocol to disable permanently ad hoc wireless sensor network this is done by consuming battery energy. These attacks are independent of specific protocol. In this we introduce a solution that protects from three problems that are stretch attack, carousal attack and battery consumption problem by using different algorithm. Introduced algorithm provides better solution than the solution given in existing system of vampire attack. The simulation results showed that the proposed algorithm performs better.

REFERENCES

1. Eugene Y. Vasserman and Nicholas Hopper, "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks" IEEE TRANSACTIONS ON MOBILE COMPUTING, VOL. 12, NO. 2, FEBRUARY 2013.
2. I. Aad, J.-P. Hubaux, and E.W. Knightly, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.
3. G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.
4. T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc. Int'l Workshop Security Protocols, 2001.
5. J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.
6. D. Bernstein and P. Schwabe, "New AES Software Speed Records," Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.
7. W.C. Cheng, C. Chou, L. Golubchik, S. Khuller, and Y.C. Wan, "A Coordinated Data Collection Approach: Design, Evaluation, and Comparison," IEEE J. Selected Areas in Comm.,vol. 22, no. 10, pp. 2004-2018, Dec. 2004.
8. A. Manjeshwar and D.P. Agrawal, "Teen: A Routing Protocol for Enhanced Efficiency in Wireless Sensor Networks," Proc. IEEE Int'l Parallel and Distributed Processing Symp., Apr. 2001.
9. A. Scaglione and S.D. Servetto, "On the Interdependence of Routing and Data Compression in Multi-Hop Sensor Networks," Proc. ACM MobiCom, 2002.
10. M. Zhao, M. Ma, and Y. Yang, "Efficient Data Gathering with Mobile Collectors and Space-Division Multiple Access Technique in Wireless Sensor Networks," IEEE Trans. Computers, vol. 60, no. 3, pp. 400-417, http://doi.ieeecomputersociety.org/10.1109/ TC.2010.140, Mar. 2011.
11. Edwin prem kumar, Baskaran Kaliapermal, Elijah blessing Rajsingh "Research issues in Wireless sensor network Applications: A Survey"- *International Journal of information and electronics engineering*,Vol 2 No 5 September 2012
12. Kazem sohraby *Applications of Sensor networks*. First edition 2012
13. Yanli Yu,Keigiu Li, Ping Li "Trust Mechanism in wireless sensor networks :Attacks analysis and countermeasures", *Journal of networks and computer applications press 2011.*
14. Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures", *Journal of Network and Computer Applications.*
15. Javier Lopez, Rodrigo Roman, Isaac Agudo, Carmen Fernandez-Gago "Trust mechanisms in wireless sensor networks: Attack analysis and countermeasures" *International Journal of information and electronics.*