International Journal of Innovative Research in Advanced Engineering (IJIRAE)
Volume 1, Issue 1 (March 2014)

Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks

Vidya.M
Department of Computer Science and Engineering,
Atria Institute of Technology, Bangalore, India
Vidya.M1389@gmail.com

Reshmi.S
Department of Computer Science and Engineering,
Atria Institute of Technology, Bangalore, India
Reshmi101@yahoo.com

Abstract— Ad hoc low-power wireless networks are an astonishing research direction in suspecting and ubiquitous computing. Preceding security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This project explores resource exhausting attacks at the routing protocol layer, which disable networks permanently by quickly draining node's battery power. These attacks are not protocol specific, but rather rely on the class properties of routing protocols. Here we find that all examined protocols are vulnerable to Vampire attacks are easy to carry out using as few as one malicious node inside sending only protocol-compliant messages. So they are difficult to detect. Here we discuss methods to alleviate these types of attacks, including a new concept protocol assured with proofs that provably bounds the damage caused by vampire attacks on nodes during packet forwarding phase.

Keywords—Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks.

I. INTRODUCTION

AD hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as continuous connectivity, ubiquitous on-demand computing power and deployable communication required instantly for first responders and military purposes. These networks already monitor factory performance, environmental conditions to name a few applications [1]. Due to their organization, these networks are particularly vulnerable to denial of service (DoS) attacks research work has been done to enhance survivability. Here, we consider how routing protocols though designed to be secure, lack protection from these vampire attacks which deplete life from these networks.

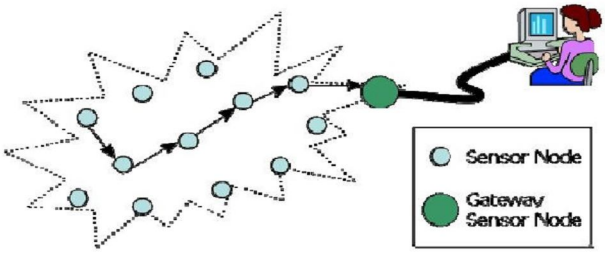

Fig. 1 Wireless Sensor Networks (WSNs).

There are three primary contributions in the paper. First, we evaluate the vulnerabilities of existing protocols thoroughly to routing layer battery depletion attacks. Second we observe that security measures to prevent these depletion attacks are orthogonal to those which are used to protect existing secure routing protocols, and its infrastructure [1].These wireless sensor networks (fig.1) offer certain enhancements and capabilities to assist in the national effort to increase alertness to potential terrorist threats as well as operational efficiency in civilian applications. Wireless ad hoc sensor networks are classifies mainly two types whether the data in the network is aggregated and whether or not the nodes are individually addressable.

A. Attacks Focused

Here we mainly focus on these attacks which are two types that are used for Denial of Service Communication.

B Carousel Attack

In this carousel attack (fig.2), a malicious node sends a packet with a composed route which as a series of loops, so that the same node would appear in the route for many times [1].

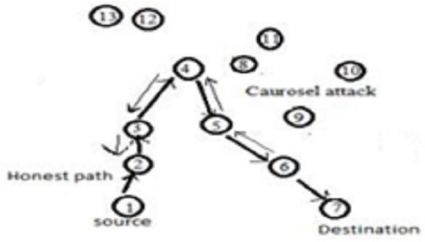

Fig. 2 shows the carousel attack same node appears in the route many times.

In this carousel attack (Fig.2), a malicious node sends a packet with a composed route which as a series of loops, so that the same node would appear in the route for many times [1]. This strategy is mainly used to increase the length of the route which is beyond the total number of nodes in the existing network, only limited by the number of entries which is allowed in the source route [5]. Example for this type of route is given in Fig.2 the thin shows the malicious path and thick path shows the honest path.

C. Stretch Attack

Another such attack in the same way is the stretch attack, where a malicious node in network constructs artificially long routes from source, which cause packets to traverse larger than optimal number of nodes [5]. In the example given below (Fig.3) honest path is shown with thick lines and adversary or malicious path with thin lines. Thus malicious path take a long distant then the honest path by making more consumption of energy.

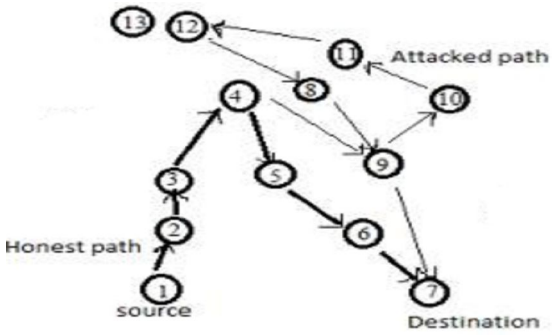

Fig. 3 shows stretch attack where malicious path takes the longest route.

In contrast to other attacks this attack shows more uniform energy consumption for all the nodes in the existing network, as it increase the length of the route, by causing more number of nodes to process the packet in the network. While vampire attacks make network-wide energy usage significantly as individual nodes are also affected noticeably till destination. Thus long routes will lose almost 10 percent of their total energy reserve per message.

II. RELATED WORK

Existing research work on secure routing protocols attempts to ensure that malicious nodes cannot cause path discovery to return an invalid network path as these nodes do not alter discovered paths but, by using existing valid paths in the network and protocol compliant messages. These adversaries mainly have limited power to affect forwarding of packets in network, making these protocols resistant to these vampire attacks. By the use of directional antenna they can consume more energy by restarting packet in various parts of the network. Other such attack is spurious route discovery where each node will forward route discovery packets which means by sending a message it is possible to cause flood attack in network.

A. Drawbacks of the existing system

1) Adversaries have limited power.
2) Security level is low.
3) Lost productivity.
4) Various DOS attacks.
5) Spurious route discovery.

III. PROPOSED SYSTEM

Nodes mainly identify by their neighbours by considering the most significant bit and they construct a tree by considering all relationships among neighbours and finally it forms a group which will be used for routing and addressing. It mainly uses No-backtracking property which it is satisfied by a given packet if and only if it makes progress towards destination in the existing network space.

A. Advantages of the proposed system

1) Highly secured authentication.
2) High efficiency.
3) No flooding.
4) Timely delivery of packets.

IV. RESULT ANALYSIS

The relationship between different components of system is shown by architecture diagram (Fig.4). This diagram gives entire analysis on concept of the system. Here each node independent of taking decisions and they identify neighbour node in the existing network. When a local broadcast message is received by the node it identifies the nearest node and forwards it to the nearest neighbour node.

Here a tree is formed by identifying the nearest neighbour nodes in the existing network .Once tree is formed the packet is forwarded by identifying shortest path among the tree which is formed by using no-backtracking property.

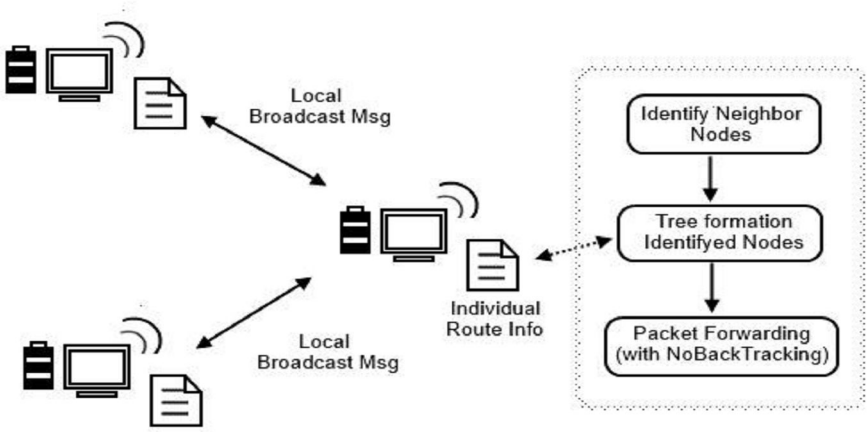

Fig. 4 Architecture Diagram.

A. Finding Neighbours

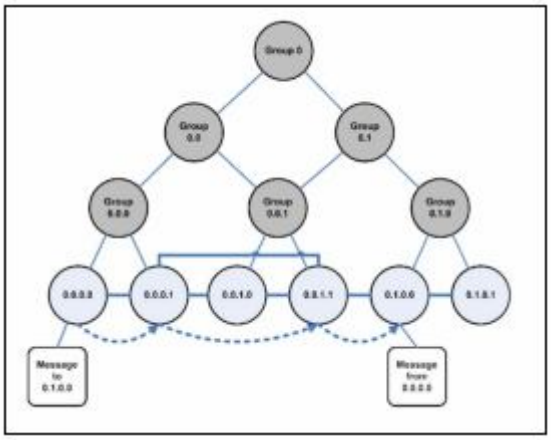

Fig. 5 Group Identification.

This module (Fig.5) is mainly used to identify the nearest neighbour node within the network. When a local broadcast message is transmitted it forwards a message to its neighbour node in the network. The neighbour node on receiving this broadcast message sends an acknowledgement to the sender node and from this acknowledgement message the sender node identifies the neighbour node. Only the neighbour nodes are involved in transmitting the message. Discovery of nodes begins with a time-limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key, signed by a trusted offline authority. Each node starts as its own group of size one, with a virtual address 0.

B. Transmission History

This module maintains a record of previous packet transmission done by each node in the network. This record mainly consists of the hop count of previous route and it keeps on updating this history through which attack immunity of our system can be improved.

C. Packet Forwarding

This module is used to transmit packet to nodes using the above formed tree structure (Fig.6). Here each node has independent route constructed from the tree structure and it also checks for the condition to match No Backtracking property or else it leads to an attack (Fig.7) (Fig.8). During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address. Thus every forwarding event shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.

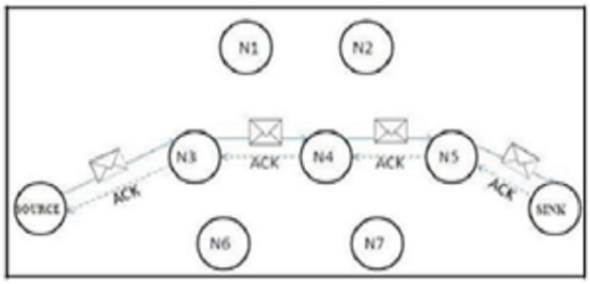

Fig. 6 Message Traversal in normal direction.

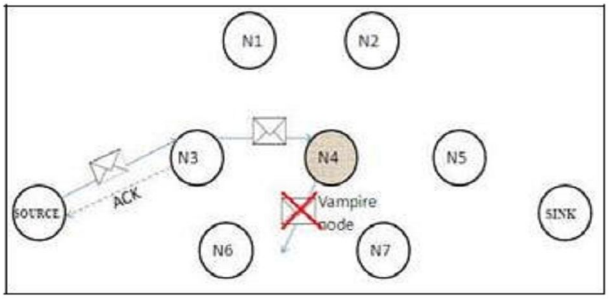

Fig. 7 Vampire Attack will lead to message drop.

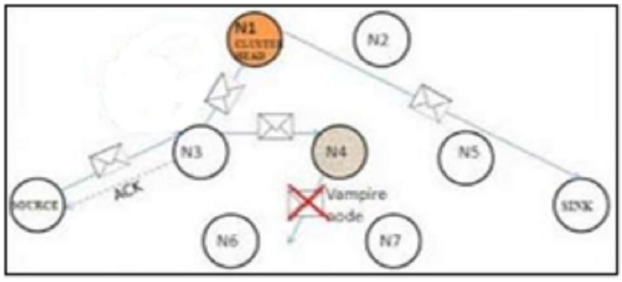

Fig. 8 After N trials node N3 sends data to cluster head
(Chosen based on highest coverage range) which sends data to sink.

D. PLGP satisfies No-Backtracking

The PLGP protocol is modified as clean state secure routing protocol such that they can resist vampire attacks during the forwarding. PLGP was vulnerable to vampire attacks even though they were said to be secured [5]. When the route discovery begins each node has a limited view about the network. As already said nodes discover the other nodes in a group by broadcasting a certificate id, signed by the public key of the online authority, thus forming a single group and a tree structure that will be used for addressing and routing [8]. PLGP protocol used for validation of packets in tree is as follows:

No-Backtracking Property

1. Function secure _ forward _address(p);
2. S←extract _ source _address(p);
3. A←extract_ attestation(p);
4. **if**(*not* verify _source _sign(p)) or
5. (empty(a) and *not* is _neighbor(s)) or
6. (*not* saowf _verify(a)) **then**
7. **return** ; /*drop(p)*/
8. **For each** *node* in a **do**
9. *Prevnode* ←*node*;
10. **if**(*not* are _ neighbors (*node* ,*prevnode*)) or
11. (not making _progress(*prevnode* ,*node*)) **then**
12. **return** ; /*drop(p)*/
13. c←closest _ next _node(s);
14. p'←saowf _append(p);
15. **if** is _neighbor(c) **then** forward(p' ,c);
16. **else** forward(p' ,next _hop _ to _ non _neighbor(c));

V. CONCLUSION

I have dedicated large part of my phases to explain Vampire Attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting node's battery power. These vampire attacks are not protocol specific but rather expose their vulnerabilities to classes of protocols. Here I have explained about PLGP protocol which is mainly based on No-Backtracking property for depletion of vampire attacks.

REFERENCES

[1] Eugene.Y.Vasserman, Nicholas Hopper, Vampire Attacks Draining Life from Ad hoc wireless sensor networks, IEEE volume 2 (2014).
[2] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.
[3] The network simulator — ns-2. http://www.isi.edu/nsnam/ns/.
[4] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.
[5] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.
[6] Daniel J.Bernstein,Synookies,1996.http://cr.yp.to/syncookies.html.
[7] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.
[8] J.W.Bos, Dag Arne Osvik, and Deian Stefan, Fast implementations of AES on various platforms, 2009.
[9] Haowen Chan and Adrian Perrig, Security and privacy in sensor networks, Computer 36 (2003), no. 10.