www.ijecs.in
International Journal Of Engineering And Computer Science ISSN:2319-7242
Volume - 3 Issue - 8 August, 2014 Page No. 7664-7667

Depletion of Energy Attacks in Wireless Sensor Networks

S Himabindhu[1], G Sateesh[2]

[1] M.Tech Student,
Department of CSE,
SVCET,Chittor,A.P.India

[2]Assistant Professor,
Department of CSE,
SVCET,Chittor,A.P.India

Abstract— *Network survivability is the capacity of a network keeping connected under loss and intrusions, which is a major concern to the design and design interpretation of wireless ad hoc sensor networks. Ad-hoc low power wireless networks are in inquisition in both discerning and ubiquitous computing. The proposed method discusses about energy draining attacks at the routing protocol layer, which drains battery power. A innovative approach for routing protocols, affect from attack even those devised to be protected which is short of protection from these attacks, which we call energy debilitating attacks, which enduringly disable networks by quickly draining nodes battery power. These energy depletion attacks are not protocol specific but are disturbing and hard to notice, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages.*

Index Terms—*Denial of service, security, routing, ad hoc networks, sensor networks, wireless*

1. Introduction

Wireless ad-hoc Sensor Networks contributes one of the mislaid acquaintances among the Internet and the physical world. One of the fundamental dilemmas in sensor networks is the computation of indemnity. Disclosure is precisely relevant to description in that it is a part of how would sensor network will observe an object, moving on an arbitrary path over a given time. A dynamic and valid method is developed for computation in sensor networks, specifically for treasuring nominal liability paths. These paths mainly contribute beneficial data about all the cases of liability-based indemnity in ad-hoc sensor networks. This algorithm will work for all given distribution of intensity models, sensor and characteristics of the network. It mainly provides an absolute level of certainty as a purpose of cache and run-time.

These attackers may dispose malicious nodes with identical or more hardware potential as the reliable nodes that might intrigue to attack the system collectively. These hackers may bring these malicious nodes by acquiring them disparately or by "dirning" a few authorized nodes by securing them and physically overriding their memory. In some cases nodes might have high- quality inter communications links available for correlating their attack. The sensor nodes may not be tinker defiant and if any attacker adjusts a node, it can extract all data, key material, and code stored on that node. So WSN has to face numerous risks that may easily obstruct its process and invalidate the assets of using its dispensation. Routing and data forwarding is a imperative maintenance for sanctioning communication in ad-hoc sensor networks.

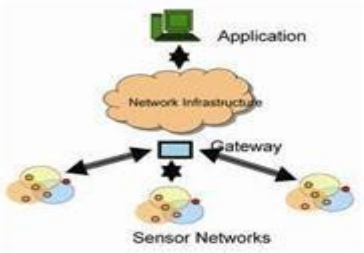

Fig. 1 Wireless Sensor Networks (WSNs).

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.

II. OVERVIEW

The immoderate resource limitations of sensor devices constitute substantial provocation to resource-aching certainty systems. The hardware curtailment entails immensely coherent security algorithms in terms of memory, bandwidth, and computation complexity. This is no superficial endeavor. Energy is the most valuable expedient for sensor networks. In terms of power communication is very expensive. In order to be energy efficient a special effort should be given to security mechanisms to make it communication efficient. A significant challenge for security mechanisms is posed for sensor networks. Simply networking from tens to thousands of nodes has proven to be a substantial

task. Providing security to these networks is equally in demand. Security mechanisms must be ascendable to very large networks to sustain communication efficiency in networks. Depending on the functions of these sensor networks, the sensor nodes may be left untended for lengthy duration of time. Here we mainly focus on these vampire attacks which are used for Denial of Service Communication. First is carousel attack, an adversary mainly composes packets with explicitly introduced routing loops in existing network. Since we call it carousel attack, as it sends packets in circles in existing network as shown in Fig. 1. It points source routing protocols by employing the limited.

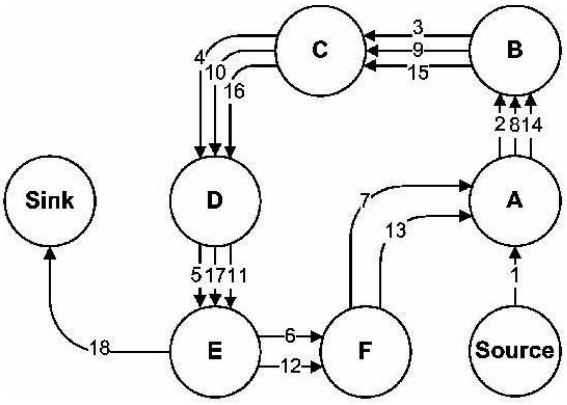

Fig. 2 shows a honest loop would exit the loop immediately from node E to sink, but malicious path makes it way twice around the loop in network before exiting it.

Second attack is stretch attack as it increment packet path lengths which cause packets to be processed by as much as possible number of nodes which is independent of hop count along the shortest path between the adversary and packet destination. An example is illustrated in Fig. 3.

In this stretch attack it mainly shows more uniform energy consumption for all the existing nodes in the network. This attack mainly lengthens the route by causing more number of nodes to process the packet in the network. These attacks mainly make use of network-wide energy usage significantly at each and every node so that they are also affected until it reach destination.

Here in this section we mainly discuss various protocols proposed by various researchers in wireless sensor networks. Here attacks have not rigorously defined at routing layer.

Thus power depletion can be found in, as "sleep privation affliction". As we explained, the proposed attack prevents nodes from entering a sleep cycle, and which leads to faster depletion of batteries.

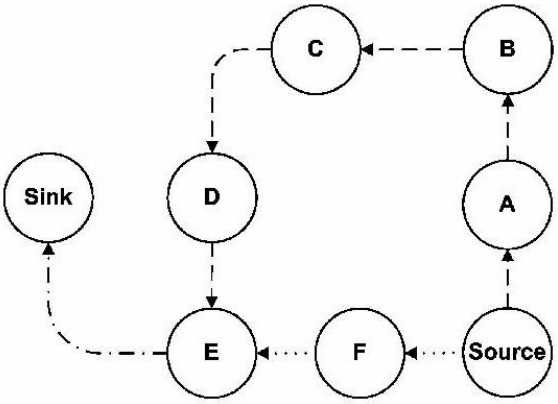

Fig. 3 shows the stretch attack where honest route is dotted and malicious route is dashed.

III. PROTOCOLS AND ASSUMPTIONS

A. Stateful Protocol and their attacks

In this protocol is where nodes are aware of their forwarding decisions, topology and its state. Here servers are supposed to recall so that it can be resumed. State and distance vector are two important classes of stateful protocols. OLSR and DSDV are examples of link-state and distance-vector. Both of these protocols are aggressive, which directs to all available nodes in the network and by decreasing the initial delay. Each node maintains a routing table which contains all accessible destinations and number of hops and next node to reach the destination and systematically send table to all of its neighbors so that it can update topology. There are mainly two types of attack they are directional antenna attack and malicious discovery attack. In this first attack the malicious have little control over the progress of packets, but they still waste their energy by restarting a packet in various parts of network. Second attack is also called as spurious rote discovery. This type of attack becomes serious when nodes claim lengthy routes have changed.

B. Stateless Protocol and their attacks

This protocol does not require the server to retain session information about each communications partner for the duration of multiple requests and its only communication protocol which treats each and every request as an independent transaction which is unrelated to any previous request so that the communication consists of independent pairs of requests and responses.

C. Clean State Secure Routing Protocol

The PLGP protocol is modified as clean state secure routing protocol which can resist these attacks during the forwarding phase. This protocol was accessible to these attacks even though they were said to be secured. PLGP consists of a topology discovery phase, which is followed by a packet forwarding phase, which has former optionally repeated on a fixed schedule to ensure that topology information stays current.

IV. RELATED WORK

We do not implicit that depletion of nodes itself is innovative, so that these vampire attacks have not been precisely depicted, decided at the routing layer. A very early mention of power exhaustion can be found in [1], as "sleep destitution torment." The proposed attack mainly prevents nodes from entering a sleep cycle with low power, and they exhaust their batteries energy faster. This work mainly has resource exhaustion at the MAC and transport layers but

also offers elimination of insider adversaries and rate limiting as probable solutions. The drawbacks of existing system is mainly adversaries have limited power and when it comes to security it's very low. There is lost productivity and there is various Denial of Service attacks.

The proposed system has nodes mainly identify by their neighbors by considering the most significant bit and they construct a tree by considering all relationships among neighbors 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. The advantages mainly has highly secured authentication and it has high efficiency and it has timely delivery of packets in the network.

V. MODULES

A. Topology and cluster head detection

The topology we have used here is a mesh topology. In this case each and every node sends a message to the other nodes which is detected in the network. Nodes maintain a record once it detects the node and this is done by using multicast socket. Based on range, battery power and mobility cluster power is detected.

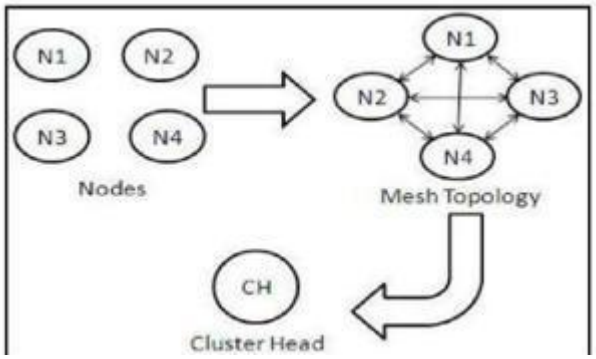

Fig. 4 Topology and Cluster Head Detection.

B. Tree formation and route discovery

Trees are formed as nodes form a group with their own identification. Here each and every node starts with their own group size as 1 and they have virtual address as 0 so that single group is established. Likewise some other groups are also established. Now as we got to know how groups are formed. In the same way two nodes form a group with their group size as 2 with one node taking a address 1 and other taking the virtual address as 0.In same way each and every group can have their own group address in the network. For Example: in group 0 node 0 becomes 0.0 and it becomes 1.0 in group 1. In such a way group is added each time or the address of each and every node is lengthened by one bit when it is merged. Thus a tree structure is formed with address in the network and node address as leaves and small groups are formed later merge to form a large group.

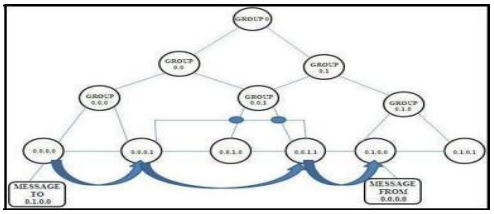

Fig. 5 Group Identification.

C. Packet Forwarding

This module is used to transmit packet to nodes using the above formed tree structure (Fig.5). 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. During this phase, each node is independently of taking decisions. Each node determines the next hop by finding the most significant bit of its address that differs from the message originator's address while receiving a packet. Thus every forwarding event shortens the logical distance to the destination, since every node addresses which is chosen should be surely adjacent to the destination. The function for forwarding of packets is as follows:

1. Function forward_ packet ()
2. so ← source _ address_ obtained (p);
3. a ← adjacent _next _node(so);
4. If is _neighbor then forward(p ,a);
5. Else
6. t ← next _ hop _to _non _neighbor (a);
7. forward (p ,t);

VI. CONCLUSION

In this paper we mainly talk about energy debilitating attacks, a new class of resource exhaustion attacks that use routingprotocols to permanently disable these networks by depleting nodes battery power in existing network. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. We also saw how to overcome these attacks by increasing the energy of the node in the network.

REFERENCES

[1] Eugene.Y.Vasserman, Nicholas Hopper, Vampire attacks Draining life from ad-hoc wireless sensor networks,IEEE volume 2 (2014).

[2] Jae-Hwan Chang and Leandros Tassiulas,Maximum lifetime routing in wireless networks,IEEE/ACM Transactions on Networking 12 (2004), no.4

[3] The network simulator — ns-2. http://www.isi.edu/nsnam/ns/

[4] Tuomas Aura, Dos-resistant authentication with client puzzles, International workshop on security protocols, 2001.

[5] John Bellardo and Stefan Savage, 802.11 denial-of-service attacks: real vulnerabilities and practical solutions, USENIX security, 2003.

[6] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

[7] I.F. Blake, G. Seroussi, and N.P. Smart, Elliptic curves in cryptography, Vol. 265, Cambridge University Press, 1999.

[8] Joppe W. Bos, Dag Arne Osvik, and Deian Stefan, Fast implementations of AES on various platforms, 2009.