International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

A SURVEY ON ATTACKS IN WIRELESS SENSOR NETWORKS ALONG WITH SCALE FREE TOPOLOGY

[1]G.Yuvasri, [2] Dr.S.Umamaheswari

[1]Student, Department of Electronics and Communication Engineering,
Kumaraguru College of Technology, Coimbatore, (India)
[2]Associate Professor, Department of Electronics and Communication Engineering,
Kumaraguru College of Technology, Coimbatore, (India)

ABSTRACT

In a densely deployed wireless sensor network ,a single node has numerous neighboring nodes with which direct communication would be possible when using moderate large transmission power this is however , not beneficial; high transmission power requires lot of energy .the recent area of WSNS has brought new challenges to developers of net-work protocols like Energy consumption ,network coverage ,node failures ,fault tolerance, network lifetime has to be preserved in wireless sensor network .This review surveys popular and efficient scale free topology which has both fault and intrusion tolerannce along with various attacks.

Keywords: Wireless sensor network, Scale-free topology, Fault-tolerance, Intrusion-tolerance, Attacks

I INTRODUCTION

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself. *keeping* data safe and secure in computers and networks became one of most interesting and challenging area in Network and Security. In spite of the fact, attackers try to achieve the sensitive and critical assets to take advantage of them. Due to many motivations, there are plenty of news about misusing information and attacking computers across the globe, which have done by intruders.

1.1 Various Kinds of Attack in Networking

1.1.1 Eavesdropping

Capturing and decoding unprotected application traffic to obtain potentially sensitive information(i.e). To listen secretly to the private conversation of othersthis is a passive attack[1], which occurred in the mobile ad-hoc network. The main aim of this attack is to find out some secret or confidential information from communication. This secrete information may be privet or public key of sender or receiver or any secrete data.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

1.1.2Data Modification

They occur when someone makes unauthorized modifications to data An attacker can modify the data in the packet without the knowledge of the sender or receiver. Data modification is a control-data-attack, which is attacker modifies the control-flow of programs. That means it corrupt user characteristics, configuration and user input data or policy making data to achieve the attacker's goals.

1.1.3 Identity Spoofing

(IP Address Spoofing) creation of Ip packets with a forged source.purpose of it is to conceal the identity of the sender (or)impersonating another computing system. the goal to flood the victim with overwhelming amount of traffic [2].It prevents an internet site (or) service from functioning efficiently or at all temporarily (or) indefinitely.

1.1.4 Denial-Of-Service Attack

Denial-of-service (DoS) attacks typically flood servers, systems or networks with traffic in order to overwhelm the victim resources and make it difficult or impossible for legitimate users to use them DoS attack as an event that diminishes or attempts to reduce a network's capacity to perform its expected function[4] . Denial of Service (DoS) is a class of attacks where an attacker makes some computing or memory resource too busy or too full to handle legitimate requests, thus denying legitimate users access to a machine[3] . There are different ways to launch DoS attacks: • Abusing the computers legitimate features. • Targeting the implementations bugs. • Exploiting the system's misconfigurations. DoS attacks are classified based on the services that an attacker renders unavailable to legitimate users.

1.1.5 Warmhole Attack

a wormhole is low latency link between two portions of a network over which an attacker replays network messages[5] . This link may be established either by a single node forwarding messages between two adjacent but otherwise non neighboring nodes or by a pair of nodes in different parts of the network communicating with each other. The latter case is closely related to sinkhole attack as an attacking node near the base station can provide a one-hop link to that base station via the other attacking node in a distant part of the network

1.1.6 Blackhole Attack

A Black Hole attack is a type of routing attack in which malicious node advertise itself as having shortest path to destination in a network by sending fake route reply to the source node[6]

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

.The black hole attack is an active insider attack, it has two properties: first, the attacker consumes the intercepted packets without any forwarding. Second, the node exploits the mobile ad hoc routing protocol, to advertise itself as having a valid route to a destination node, even though the route is spurious, with the intention of intercepting packets.

1.1.7 Man-In-The-Middle Attack

MITM attack works in such a manner that it makes the users difficult to understand if they are connected to the actual secure connection or to a similar non-secure connection. When the user tries to establish a connection with the network, the user first sends packets which include the information about the user device to the necessary network. The network then creates a digital certificate which includes the encrypted connection key and the user device address. Since the certificate that is being passed during the connection initialization is insecure, the attacker can easily gain access to the digital certificate and modify the information in the certificate leaving the approval of the certificate to the user[7]. Many users do not have enough knowledge to check about the whereabouts of the forged and duplicate certificates and the attacks corresponding to them, thus they accept the certificates and allow connection to the non-secure network making way for the attackers to implement the attack.

II SCALE FREE TOPOLOGY

The Fig .1. shows scale free topology for wireless sensor networks. In the figure Ro represents the nodes in first circle, Ro+t represents the nodes in second circle, n is the node joining network , 0 is the node out of network .

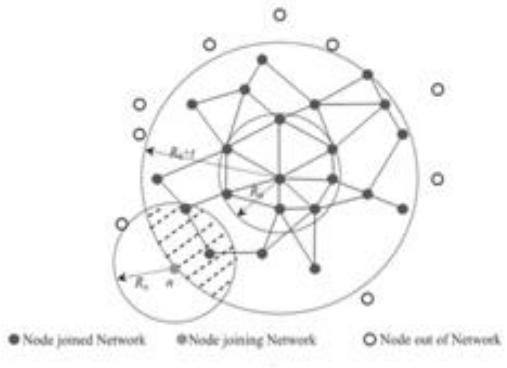


Fig. 1 Scale Free Topology

Based on the growth and preferential model nodes are placed where,

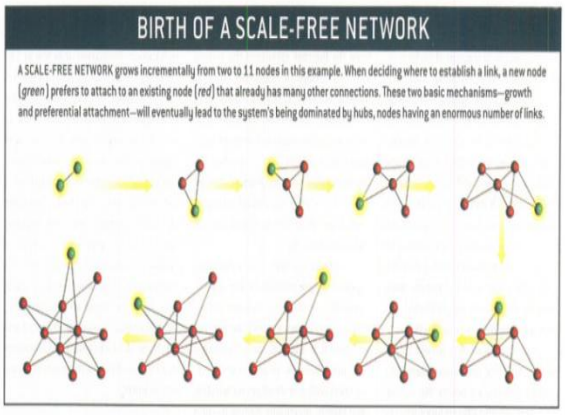
- Growth - indicates the increase in number of nodes in network with time.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

- Preferential - indicates more connected nodes receive more links.

Over the certain several years, researchers have uncovered scale-free structures in a stunning range of systems[8]. When we studied the World Wide Web, we looked at the virtual network of Web pages connected to one another by hyperlinks. Researchers have also discovered that some social networks are scale-free. Collaborations between scientists from Boston University and Stockholm University, for details, has shown that a network of sexual relationships among people in Sweden followed law: although most individuals had only a few sexual partners during their lifetime, a few (the hubs) had hundreds. A recent study led by Stefan of the University of Kiel in Germany concluded that the network of people connected bye-mail is likewise scale free. Sidney Redner of Boston University determined that the network of scientific papers, connected by citations, follows a power law as well. And Mark New man of the University of Michiganat Ann Arbor examined collaborations among.

A scientist in several disciplines, including physicians and computer scientists, and found that those networks were also scale-free, corroborating A study we conducted focusing on mathematicians and neurologists.



The scale free topology is proven to be robust when attacked by random faults, but it is fragile when confronted with selective remove attacks. We propose a new scale free topology model[9]. which has both fault tolerance against selective remove attacks.

III PROPOSED WORKS

- Scale-free topology model
- Degree distribution characteristics
- Mathematical optimization model

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

3.1 Scale-Free Topology Model

In order to evolve the scale-free topology with the good performance of both fault-tolerance and intrusion-tolerance in WSNs, we can use the improved growth and preferential attachment to build the scale-free topology model with the local-area idea. Then the evolutional degree distribution of the model is discussed.

3.2 BA-E Evolution Model

In, BA model uses the method of growth and advantageous attachment. In the growth process, the number of nodes in the network grows continuously[4]. In the preferential attachment process, the probability of a new node to be linked to an existing node i depends on the degree k i of nod e i, and obeys the following rules

$$\prod(k_i) = \frac{k_i}{\sum_j k_j}$$

The growth rule and preferential attachment rule above lead to a skewed degree distribution for topology, it build ups the BA scale-free topology whose degree distribution follows $p(k) \propto k^{-3}$.

The evolution of BA-E model the initial network consists of m0 nodes and e0 links. It is supposed that, node n joins the network at time t, R n is the transaction radius of node n, R0 is the initial network radius, R0+t is the network radius at time t. Considering the degree disposal of BA-E model, the probability that the node n builds communication link in its local-area is decided by Eq. and m new links are formed during each time. According to the mean-field theory, we get

$$\frac{\partial k_i}{\partial t} = m \prod_{local}(k_i)$$

within $[3,+\infty)$ by adjusting the parameter p.When $p \to 0$, we can get $p(k) \sim k^{-3}$, then the degree distribution of BA-E model is closing in on the BA scale- free topology which has the good capability of fault-tolerance against random faults; when$p \to 1$, we can get $p(k) \propto e^{-k/m}$, then the degree distribution of BA-E model is closing in on the random topology which has the good capability of intrusion-tolerance across selective remove attacks.

3.3 Mathematical Optimization Model

Based on the analysis of the degree distribution of BA-E model, the topology derived by BA-E model exist the optimal value p (which can withstand node failures, that is, the random faults and the selective remove attacks). In this section, we analyze the effect of degree distribution aspects on topological fault-tolerance and topological intrusion tolerance, then find the optimal p. Base do n p, an optimal BA-E scale-free topology is derived which keeps the topological fault-tolerance and maximizes the tele-logical intrusion-tolerance.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

3.4 BA-E Fault-Tolerance Index

Based on the percolation theory, Cohen et al. have studied the properties of the percolation phase transition, and found that there is a critical point evacuation ratio hr, and hr can be used as the fault-tolerance strength criterion of the scale free topology. When the removal ratio of random nodes is more than hr, the topology will collapse into many smaller disconnected parts. And Ref. applied a general criterion for the existence of a spanning part, and this criterion can be written as

$$\frac{\langle k^2 \rangle}{\langle k \rangle} = 2$$

When an h(0<h<1) ratio of nodes is randomly removed, for a node with initial degreek0chosen from an initial distribution p(k0), the connectivity distribution of the node is changed from the original distribution p(k0) to a new distribution ˜ p(k).

IV CONCULSION

In this paper we focus on some of the common attacks like eavesdropping, man in middle attack, black hole, warm hole, data modification ,identity spoofing, Denial of service. As we have discussed, it is found that the man in middle attack has quite interesting features compared to other attacks. In future, the idea is to insert the man in middle attack in scale free topology of placing nodes in WSN. Further this paper provides information about scale free topology.

REFERENCES

[1].D. Kapetanovic, G. Zheng, F. Rusek, "Physical layer security for massive MIMO: An overview on passive eavesdropping and active attacks", *IEEE Commun. Mag.*, vol. 53, no. 6, pp. 21-27, Jun. 2015.

[2] F. Guo and T. Chiueh, “Sequence Number-Based MAC Address Spoof Detection,” Proc. Eighth Int’l Conf. Recent Advances in Intrusion Detection, pp.309-329

[3] A. D. Wood and J. A. Stankovic, 2002 "Denial of service in sensor networks, " *Computer*, vol. 35, pp. 54-62

[4]Q. Yan, F. Yu, "Distributed denial of service attacks in software-defined networking with cloud computing", *IEEE Commun. Mag.*, vol. 53, no. 4, pp. 52-59, Apr. 2015

[5]C. Karlof and D. Wagner, “Secure routing in wireless sensor networks: Attacks and countermeasures”, In Proceedings of the 1st IEEE International Workshop on Sensor Network Protocols and Applications, May 2003, pp. 113-127. (ACM-SE'42),.

[6] M. Al-Shurman, S.M. Yoo, S. Park, “Black Hole Attack in Mobile Ad Hoc Networks”, 42nd Annual ACM Southeast Regional Conference .

[7]G. Nath Nayak, S. G. Samaddar, "Different flavours of man-in-the-middle attack consequences and feasible solutions", *Proc. 3rd IEEE Int. Conf. Comput. Sci. Inf. Technol. (ICCSIT)*, vol. 5, pp. 491-495, 2010.

[8] Holme P, kim BJ. Growing scale-free networks with tun2006 able clustering. Phys Rev E 2002;65:026107

[9] Yin RR, Liu B, Liu HR, Li YQ. The critical load of scale-free fault-tolerant topology in wireless sensor networks for cascading failures. Physica A 2014;409:8–16

[10] Peng GS, Wu J. Optimal network topology for structural robustness based on natural connectivity. Physica A 2016;443:212–20

[11] Barabasi AL, Ravasz E, Vicsek T. Deterministic scale-free networks. Physica A 2001;3-4:559–64

[12] Bari A, Jaekel A, Jiang J, Xu YF. Design of fault tolerant wireless sensor networks satisfying survivability and lifetime requirements. Comput Commun 2012;35:320–33.

International Journal of Electrical and Electronics Engineers
Vol. No. 9, Issue No. 01, January-June 2017
ISSN (O) 2321-2055
ISSN (P) 2321-2045

Attack name	Attack definition	Attack effects
Eavesdropping	Overhearing the communication channel to gather confidential data	• Reduces data confidentiality • Extracts vital WSN information • Threatens privacy protection of WSN
Black hole	Attracting all the possible traffic to a compromised node. Can result in launch of other attacks.	,• Triggers other attacks like wormhole,eavesdropping Exhausts all the network resources • Packet dropping/ corruption • Modification of routing information
Denial of Service (DoS)	Prevents the user from being able to use the network services. Extends to all the layers of protocol stack	▪ . Reduces WSN availability Affects physical layer, link layer, network layer, transport layer and application layer ▪ Prevents access to network services by the user
Wormhole	Tunneling and replaying messages from one location to another via low latency links that connect two nodes of WSN	. Changes normal message stream • False routes / misdirection • Forged routing • Changes network topology
Man in middle attack	occurs when the attacker manages to position themselves between the legitimate parties to a conversation.	➢ Able to read and alter the intercommunication ➢