IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

Enhancing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack

Sapna Yadav[1], Nilesh Sambhe[2], Vikas Palekar[3]

Department of Computer Technology, YCCE, Nagpur, Maharashtra, India[1,2]

Department of Computer Science and Engineering, DMIETR, Wardha, Maharashtra, India[3]

Abstract: Network survivability is the ability of a network getting connected under failures and attacks, which is the most important topic in the design and performance of wireless ad hoc sensor networks. The motivation of a large portion of research efforts has been to increase the network lifetime, where the lifetime of network is measured from the instant of deployment to the environment when one of the nodes has exhausted its limited power source and becomes in-operational which is commonly referred as first node failure. But there is a class of resource consumption attack called vampire attack whose work is to permanently disable the whole network by quickly draining nodes battery. The paper projects its focus on the way in which the attack should be overcome in the best possible manner. The security work in the wireless sensor network area which is priority and primarily focusing on denial of communication at the routing or mac levels. In this paper, the attack which is mainly focusing on the routing protocol layer that type of attacker is known as the resource depletion attacks. This attack causes the impact of disabling the networks by drastically draining the nodes battery power. This paper presents the detecting and preventing the lifetime of node by vampire attack and also the data security using the secret sharing algorithm.

Keywords: wireless sensor network, AODV, secrete sharing algorithm, DOS, MAC.

I. INTRODUCTION

A. Background and Motivation

Ad hoc wireless sensor networks promise to be good new applications in the near future, such as continuous connectivity and demanding the computing power and deployable communication required instantly for first responders and military purposes. These networks are already monitor factory performance, environmental conditions to name a few applications. Due to the organization of these networks are particularly vulnerable to denial of service (DOS) attacks research work has been done to enhancing the survivability. Low-power wireless networks are an exciting research direction in the sensing and pervasive computing.

Prior Security work has focused primarily on denial of communication at the routing or mac levels. So the reduction in the resource attacks at the routing protocol layer, which permanently disables networks by fast draining node's battery power. These vampire attacks are not specific to any defined protocol, but rather rely on properties of many popular classes of routing protocols.

These vampire attacks are devastating and it is very difficult to detect, and it is achieved without great effort to carry out using as few as one malicious insider sending only protocol-complaint messages. In worst case, vampire can increase network wide energy usage by a factor of O (N), where N is the number of network nodes.

Routing in sensor networks is very provocative due to several characteristics that distinguish them from contemporary communication and wireless ad-hoc sensor networks.

Firstly, it is very difficult to build a global addressing scheme for the deployment of sheer number of sensor nodes. So that the IP-based protocols can't be applying to sensor networks. Secondly, in direction of typical communication environment, almost all applications of sensor networks require the flow of sensed data from multiple regions (sources) to the sink. Third, generated data traffic has significant redundancy in it since many sensors may generate same data again and again within the particular place of a phenomenon. Such redundancy is important to be exploited by the routing protocols to

Increase energy and bandwidth utilization. Fourth, sensors are tightly constrained in terms of power, on-board energy, processing capacity and storage and thus want careful resource management. Due to such differences, many algorithms has been proposed for the problem of depletion of energy in sensor networks.

Types of Attack

Carousel Attack: In this carousel attack a malicious node sends a packet with a composed route which as a series of loops, that's why the same node would appear in the route for number of times. In the Carousel attack, attackers introduce many packet within a route tranquil as a sequence of loops, so that the same node appears in the route of communication more than once.

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

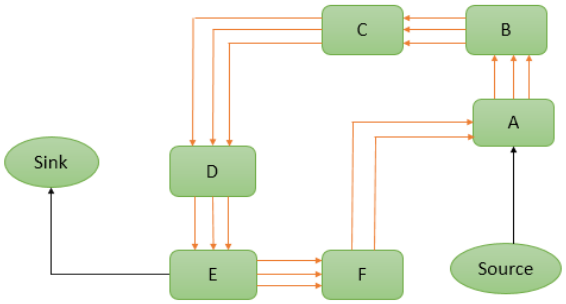

Fig: Carousal attack

Stretch Attack: This attack also targeting resource steering, attackers constructed the falsely long routes, potentially traversing each and every node in the network. Also stretch attack, increases packet lane length, causing packets to be processed by many of nodes that is governing by itself of hop count down the straight path stuck between the challenger and packet target.

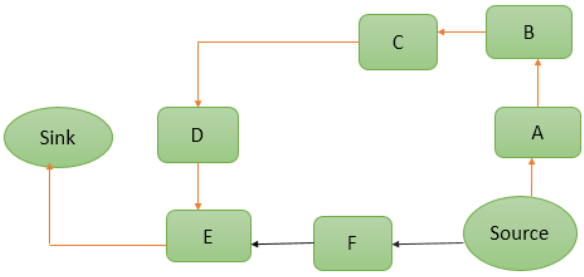

Fig: Stretch attack

B. Limitation of Prior Work

Previous work on Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by preventing Vampire Attack was using PLGPa protocol.[A. Vincy, and Uma Devi, (2014)]The basic idea of PLGPa was to provably bounds damage from vampire attacks by justifying the packets towards the destination. It was the first sensor network routing protocol. But the depletion of attack in this work is not predicted. If the message received at sink is original it can be saved and preserve.

In case, attack is terminated at any of the nodes in travelling path then the message is corrupted and moves into a malicious packet. In PLGP, forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any node of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks.

C. Attack on various kind of protocol

Assume there are numbers of people communicating in the world, they use various types of languages, and the various machines, the number of ways in which they transmit data and the different software also they use. We would never be able to communicate with the whole world if there were no standards way in which we communicate and the way our machines treat data. These standards are nothing but a sets of rules. There are rules conduct how data is transferred over networks, how they are compressed data into a small space, how they are presented on the screen and so on. These set of rules are called protocols [1]. There are many protocols, each one conduct the way a certain technology works. For example, the IP protocol gives a set of rules which conduct the way computers use IP packets to send data on the Internet.

II. ATTACKS DETECTION

We consider three DoS attacks. First, we propose an AODV protocol for detecting Dos attacks. Second propose an Encryption/Decryption algorithm for verifying the file and implement attack removal mechanisms. We implemented our Protocol and conducted extensive experiments on both real and synthetic policies. The results shown aodv sends out periodic routing updates at every 90 seconds. In this attack detection we organize the paper as follows. In section I significant usage of wireless network and resource draining attacks on network along with its related work discussed. In section III we give methodology of the concept. The evaluation parameter discussed in section IV. In section V Experimental results is shown. We conclude the aodv timer and loop avoidance for detecting vampire attacks Using periodic routing updates at every 90 seconds in Section VI. In final we give reference to successfully done this paper.

III. RELATED WORK

A Vincy [1] suggested that the protocols developed to protect from DOS attack, but it is not completely possible. So they work on the DOS attack i.e. Vampire attack-loosing of node's life from wireless ad-hoc sensor networks. The data verification process is provided at both server and client side. It provides comparatively high security. It reduced the intruder spoofing. In this paper, they concentrate on the energy efficient protocols in which they divide the network to efficiently maintaining the energy consumption of sensor nodes and perform data aggregation and fusion in order to decreases the number of transmitting the messages to the sink. Those have been developed for wireless sensor networks.

Eugene Y. Vasserman [2] explores resource depletion attacks at the routing protocol layer, which permanently damage the networks by fast draining nodes battery power. They find that all examined protocols are susceptible to Vampire attacks, which is devastating hard to detect and it is easy to carry out using as few as one malicious insider sending only protocol compliant messages. They showed a number of proof-of-concept attacks against representative the example of existing routing protocols using a small number of weak adversaries.

Ambili M.A [3] define that a Network survivability is the ability of a network keeping connected under failures and attacks, which is the main important issue in the design and performance of wireless ad hoc sensor networks. This paper focus on the way in which the attack can be overcome in the best possible manner. An energy

DOI 10.17148/IJARCCE.2016.54103

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

constraint intrusion detection Schemes are introduced along with clean state secure routing protocol.

Vidya M. [4] explores resource draining attacks at the routing protocol layer, which disable networks permanently by fast draining node's battery power. Here they discuss methods to alleviate these types of attacks, including a new concept of protocol assuring with prove that can hold the damaged causing by the vampire attacks on nodes during packet forwarding phase. Here they have explained about PLGP routing protocol which is mainly based on No- Backtracking property for depletion of vampire attacks.

Xiao-Min Hu [5] presents the maximizing the lifetime of a sensor network by scheduling operations of sensors is an effective way which construct energy efficient wireless sensor networks. This paper proposes a hybrid approach of combining a genetic algorithm with the schedule transition operations, termed STHGA, to address the problem of depletion of energy in the network.

K.Vanitha [6] presents the evaluation of the vulnerabilities of existing protocols, Quantization of performance of various protocols that exist in the solitary vampire and Modification of existing protocol to deplete vampire attacks. A new of energy class that draining the power of nodes which use routing protocols to permanently halt ad hoc wireless sensor networks which can depleting the nodes' battery power.

E.Mariyappan [7] presents the existing secure routing protocols such as SAODV and SEAD do not protect against vampire attacks. A wireless sensor network encryption protocol using boundary recognition technique is introduced to prevent an instance of resource depletion attack by the recursive grouping algorithm and jump point algorithm so that an accurate path is produced to prevent the vampire attacks during packet transmission case.

Lina R. Deshmukh [8] presents a new proof-of-concept protocol is a method which can be discussed to mitigating these kinds of attacks. The protocol limits the damage caused at the time of packet for transmission done by Vampires. To diminish the Vampire attacks using PLGP-A identifies malicious attack, in which certain approaches are also discussed.

ManjuV.C [9] explore resource's depletion attacks on the routing protocol layer and packet forwarding in which invariably disable networks by quickly draining the nodes power, is called as Vampire Attack. In this, attacks are not any protocol design, but rather depend on the properties of the many classes of routing protocols. So they work on routing protocol.

IV. WORK METHODOLOGY

The work is done for discovery of vampire i.e. malicious node and removal of malicious node and the security in transmission by using the routing protocol which gives the better result i.e. the work is explain in three phases. First phase describe that when the source node send the data in the encrypted form by using the secret sharing algorithm to gives the higher security for the data. Second phase describe that the detection of vampire attack i.e. the scanning of the network for the 90 second to know the energy of the nodes present in the network if it is found that the vampire attack is present in the network than the removal of vampire attack is done. Third Phase describe that if the vampire attack is not present in the network than it will set the path using AODV routing protocol than receiver decrypt the data using the secret sharing algorithm and then receiver get the original packet.

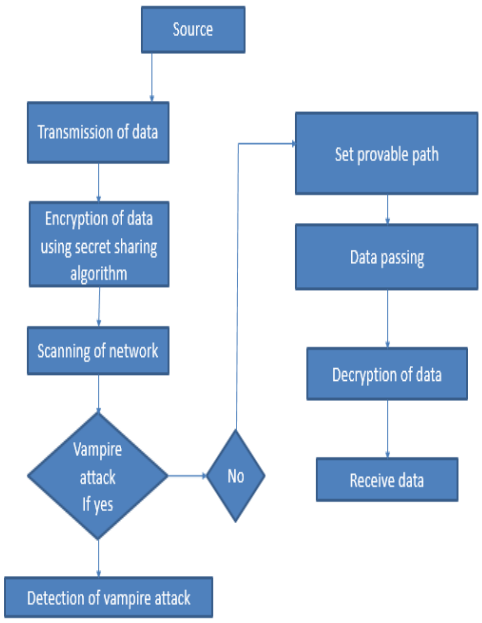

Fig: Flow diagram

V. EVALUATION PARAMETER

Analysis of energy attacks is performed using the Dot net. In this, the experimental model is built on 18 nodes which can be increased further up to 1000 distributed randomly. The sensor nodes operate on non-renewable batteries and start the process in which initial energy equal to 4J. Each node uses its limited reserves of energy throughout the duration of experimentation. Thus, any node which has exhausted its energy reserve is considered as dead node. Therefore, it can't transmit or receive data. The experimental parameters used in the model are summarized in the table below.

Parameter	Value
Channel type	Wireless channel
Network interface type	Physical/ Wireless Physical
MAC type	Mac/802_11
Routing protocol	AODV
Initial energy in Joule	100 J

DOI 10.17148/IJARCCE.2016.54103

IJARCCE

ISSN (Online) 2278-1021
ISSN (Print) 2319 5940

International Journal of Advanced Research in Computer and Communication Engineering
Vol. 5, Issue 4, April 2016

A. Implementation techniques

Secret sharing Algorithm: In cryptography, the secret sharing refers to a method for distributing a secret amongst a group of participants, each of which is given a share of the secret. The secret can only be reconstructed when the shares are combined together; individual shares are of no use on their own. Gives tight control and removes single point vulnerability. Individual key share holder cannot change/access the data.

Example:

- Goal is to divide some data S (e.g., the safe combination) into n number of pieces S1, S2….Sn in this way:
- Information of any k or more S pieces makes S easily computable.
- Information of any k -1 or pieces leaves S completely undetermined (in the sense that all its possible values are equally likely).
- This scheme is also called (k, n) threshold scheme. If k=n then all participants are required together to construct the secret again.
- Suppose we want to use (k, n) threshold scenario to share our secret S where k < n.
- Choose at random (k-1) coefficients b1, b2, b3…bk-1, and let S be the b
- Construct n points (i, f (i)) where i=1, 2…..n
  Given any subset of k of these pairs, after that we can find the coefficients of the polynomial by interpolation, and then evaluate b0=SS, which is the secret.

VI. EXPERIMENTAL RESULT

We evaluate the efficiency of our protocol on both presence and absence of attacks. We implemented our protocol using Dot net. Our experiments were carried out on a PC running Windows 7 with 20GB of memory. We define a vampire attack as the constituents and transmission of a message that causes more energy to be consumed by the network than if a node which is not a malicious transmitted a message of identical size to the same destination, although using different packet headers. So that we measure the strength of the attack by the ratio of network energy used in the beginning case in which the energy used in the malicious node case, i.e. the ratio of network-area power utilization with malicious nodes present to energy used with only to the honest nodes when the number and size of packets sent remain same. Safety from Vampire attacks implies that this ratio is 1. The attacks are carried out by a randomly-selected opponent using the least intelligent attack strategy to obtain average damage estimates .Hence more intelligent adversaries using more information about the network which would be able to increase the strength of their attack by selecting destinations designed to maximize energy usage. As expected, the carousel attack causes excessive energy usage for a few nodes, since the nodes which are along a shorter path are affected. In contrast, the stretch attack shows that is the more uniform energy consumption for all nodes in the network, since it increases the route, causing more nodes to process the packet. While both attacks significantly network-area energy usage, individual nodes are also affected, with some losing almost 10% of their total energy reserve per message.

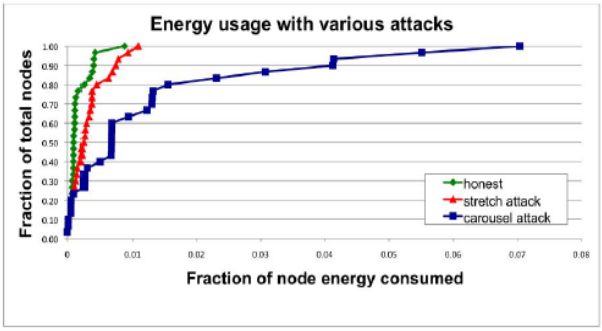

Fig: Node energy distribution under various attacks scenario [3].

Mitigation methods to prevent attacks.

The carousel attack can be prevented by forwarding nodes check source routes for loops. When a loop is detected, the source route could be detected and the packet sent on again, but one of the attractive features of source routing is that the route can be self-signed by the source. Therefore, it is better to simply drop the packet, by considering that the sending node is like a malicious (honest nodes should not introduce loops). An alternate solution is to alter how mediator nodes are process the source route. To forward a message, a node must determine the next hop by locating itself as the source route. If a node searches for itself from the destination backward instead from the source forward, any loop that includes the current node will be terminated automatically(the last instance of the local node will be found in the source route rather than the first one). No other processing is required for this defense.

The stretch attack is very challenging to prevent. Its success rests on the forwarding node not checking for optimality of the route. If we call the no-effective case strict_ source routing, since the route is followed exactly as specified in the header, we are defining loose source routing, where intermediate nodes may replace by the part or all of the route in the packet header if they know more better route to the destination. This makes it necessary for nodes to discover and cache optimal routes to a fraction of other nodes, partially defeating the as-needed discovery advantage.

a) **Formation of network phase**

This is the module of network formation in which the 18 nodes are present which can communicate with each other. When the source node send data packet to the destination through the greedy forwarding algorithm. Then the greedy forwarding algorithm do not get the data packet back to the same node and the initial energy of the node is 100 J.

b) **Communication phase**

When we click on to the browse button then it gives message that click on the secure communication button to

transmit the data packet secure to the destination. The original data is encrypted by the secrete sharing algorithm and for the communication nodes choose the shortest path to reach to the destination node. At the first when the nodes communicated the initial energy. Then it gives the energy of the nodes through which it send the packet. The energy calculation is done on the basis of the weight of the nodes. When source node is send data to the next node, the next node search the next node which has the minimum weight then it calculate the weight and send the data to the next to. In this way the scenario of transmission of data packet is done.

Comparative Analysis:
Here we are comparing the secret sharing algorithm with the AES algorithm to know that which of the algorithm show the better complexity in which the data packet is encrypted and decrypted by both the algorithm. So that we get the result that the secret sharing algorithm have taken 5 millisecond to reach to the destination otherwise the AES algorithm takes 7 millisecond to reach to the destination. Now by analyzing these result we can say that the secret sharing algorithm is better than the AES algorithm.

Next comparison is done between the attacks to know that how much energy is drain after communication i.e the secure communication, carousel attack and the stretch attack in which the secure communication is drain energy minimum as compared to carousel and stretch attack.

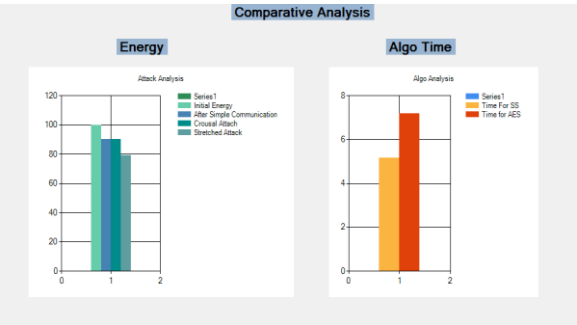

Fig: Comparative analysis

VII. CONCLUSION

In this paper, a work being done in the area of wireless sensor network to detect the vampire attack. Ad-hoc sensor network in which the routing data in them is a significant research area. There are a lot of protocols developed to protect from DOS attack, but this attack is not completely possible. One such DOS attack is vampire attack-draining of the nodes life from wireless ad-hoc sensor networks. This explores gives the resource draining of energy of the attacks at the routing protocol layer, which disabling the networks by fast draining the nodes' battery power. The position based routing protocol is an energy efficient mechanism where only the minimum processing is done by the sensor node. The experimental results show that depending on the location of the adversary, use of energy during the forwarding phase increases from between 50 to 1,000 percent. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

REFERENCES

[1] A. Vincy, and Uma Devi, "Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by preventing Vampire Attack", IEEE International Conference on Innovations in Engineering and Technology, 21st& 22nd Mar 2014.

[2] Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: draining life from wireless ad-hoc sensor networks", IEEE Trans on mobile computing vol.12 no.2 year 2013.

[3] Ambili M.A, Biju Balakrishnan, ''Vampires attack: Detection and elimination in WSN", IJSR Vol- 3 April2014.

[4] Vidya.M and Reshmi.S, "Contending Against Energy Debilitating Attacks in Wireless Ad Hoc Sensor Networks'', IJIRAE vol. 1. Mar 2014

[5] Xiao-Min Hu, Jun Zhang, "Hybrid Genetic Algorithm Using a Forward Encoding Scheme for Lifetime Maximization of Wireless Sensor Networks", IEEE TRANSACTIONS ON EVOLUTIONARY COMPUTATION, VOL. 14, NO. 5, OCTOBER 2010

[6] K.Vanitha,V.Dhivya, ''A Valuable Secure Protocol to Prevent Vampire Attacks In Wireless Ad Hoc Sensor Networks", 2014 IEEE International Conference on Innovations in Engineering and Technology (ICIET'14) On 21st & 22nd March Organized by K.L.N. College of Engineering , Madurai, Tamil Nadu, India.

[7] E.Mariyappan," Power Draining Prevention in Ad-Hoc Sensor Networks Using Sensor Network Encryption Protocol", ICICES2014 - S.A.Engineering College, Chennai, Tamil Nadu, India

[8] Lina R.Deshmukh,"Ensuring an Early Recognition and Avoidance of the Vampire Attacks in WSN using Routing Loops" 2015 IEEE International Advance Computing Conference (IACC)

[9] ManjuV.C," Detection of Jamming Style DOS attack in Wireless Sensor Network", 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing.

[10] ManjuV.C," Detection of Jamming Style DOS attack in Wireless Sensor Network", 2012 2nd IEEE International Conference on Parallel, Distributed and Grid Computing

[11] Maneesha V. Ramesh, Aswathy B. Raj and Hemalatha T," Wireless Sensor Network Security: Real-Time Detection and Prevention of Attacks", 2012 Fourth International Conference on Computational Intelligence and Communication Network

DOI 10.17148/IJARCCE.2016.54103