Analysis of Attacks in Wireless Adhoc Sensor Networks

Kannan.S[1], Palanisamy.A[2]

[1,2]*Department of computer science and Engineering*

Sardar Raja College of Engineering, Alangulam

[1]kannan17.techno@gmail.com ,[2]apalanisamy80@gmail.com

***Abstract*— Ad-hoc Wireless Networks are used extensively in pervasive computing. The attacks witnessed mainly in the areas of routing layer. The entire resource is depleted at the routing layer through vampire attacks in which the battery power of the root node is absorbed. The attacks are not specific to a particular protocol. It is harder to detect in such a way a single malicious may encounter serious problems. The draining battery power of nodes rises to drop of packets that are transferred in adhoc fashion. In this paper we analyze various possible attacks that take place in wireless adhoc sensor networks. The proposed algorithm helps in the efficient identification of vampire attacks. The mechanism used in the algorithm helps in identifying the vampire nodes which is hard to detect in the wireless adhoc sensor environment.**

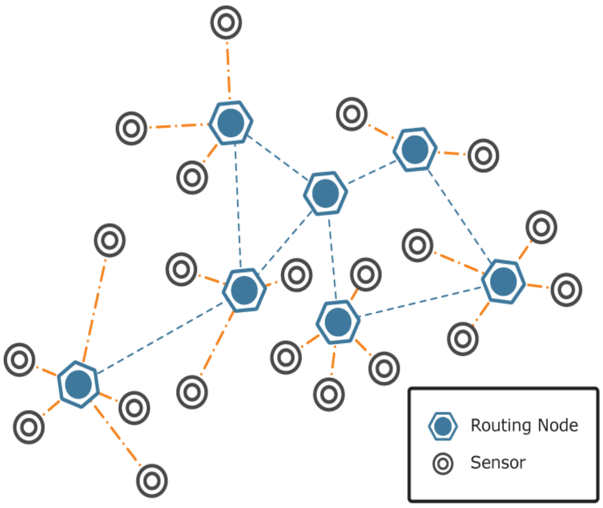
***Keywords*— loop node attack, long route attack, vampire attack**

I. INTRODUCTION

Ad-hoc wireless Networks are deployed in a wide range which makes it more popular. The wireless network encounters a immense outage in various fields which also resulted in various affecting factors over it. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable—lack of availability can make the difference between business as usual and lost productivity, power outages, environmental destruction, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. Due to the ad hoc organization, wireless ad hoc networks are especially endangered to denial of service (DoS) attacks, and a great deal of research has been done to enhance survivability While these schemes can prevent attacks on the short term availability of a network, they do not specify attacks that affect long-term availability—the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an occasion of a resource accounting attack, with battery power as the resource of interest. In this consider how routing protocols, even that draft to be secure, deficiency of protection from these attacks, which call Vampire attacks, since they evacuate the life from networks. nodes. All these attacks are different from formerly studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely weaken a network. Some of the discrete attacks are simple, and power evacuating and resource fatigue attacks have been discussed before prior work has been mostly confined to other levels of protocol stack, e.g., application layers, or medium access control(MAC) and no rigorous analysis or alleviation, of routing-layer resource fatigue attacks. DoS is a common attack experienced in wireless sensor network. Efficient mechanisms were proposed to prevent stretch attack. In addition to that various attacks affecting the routing layer are described in this paper. Some of the attacks are powerful hard to identify and involved in the delay of transmission of packets from source to destination. Among them some attacks deplete the energy of the nodes involved in the networks. This paper makes contributions in order to analyse the attacks in wireless sensor networks and discuss the measure by which these type of attacks are mitigated.

II.OVERVIEW

Attacks on wireless adhoc sensor networks may use both stateless protocols and stateful protocols. In stateless protocols the entire route to the destination is specified in the packet header by the source node. The intermediate nodes present in between source and destination does not make forwarding decisions on its own. Here the entire routing decision is done by the source node itself. To forward a packet from one intermediate node to other is already specified in the packet header. In stateful protocols forwarding decisions are based on the stored state of the network nodes. The important stateful protocols are link-state and distance-vector. Link-state networks and distance-vector are built in dynamic manner from independent forwarding decisions there by effective against the attacks takes place in stateless protocols. Fig. a shows the architecture of wireless adhoc sensor networks. In which routing layer along with the nodes are specified. The attacks maybe on the sensor nodes either similar to stateless or stateful protocols. The possible attacks on stateless protocols are loop node attack and long route attack. In stateful protocol these types of attacks are eliminated since the routing decisions are made dynamically. Even through loop node and long route attack are eliminated in stateful protocols it suffers from a attack called vampire attack. In vampire attack energy of the node are drained by malicious node, there by the drained node losses its battery power and hence the packets are neither received nor transfer the packets to other nodes. The entire routing topology is interrupted leads to packet drop.



a. Architecture of WASN

III.ATTACKS ON SOURCE ROUTING PROTOCOLS

The source routing protocols make the packet forwarding decisions by the source rather than the intermediate nodes. The routing burden entirely depends upon the source for transmitting packets. The loop node attack and long route attack makes the energy consumption to a great extent. These types of attacks by the malicious node affect the transmission over the network.

A .Loop Node Attack:

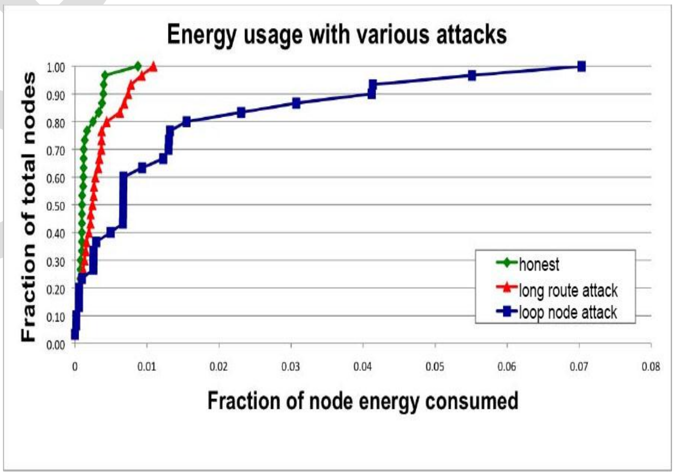
In loop node attack the malicious node sends a packet with a route that comprises of series of loops in such a way that same node appears in the route for many times. By repeating the same node again and again in the route the number of nodes to traverse automatically increases. The length of the route is increased by the malicious node. When the same node is repeated as many times in the route the energy needed to reach the destination increases. In source routing protocols the nodes in between are not aware about the routing. The source node is entirely responsible for the packet transmission. If the source node is malicious then the entire routing decisions would result in the false transmission rate. The energy usage drastically increases with the number of nodes visited. The malicious node limits the transmission rate to avoid the saturating the network, the energy usage of this attack increase by a factor of O(n) where n is the maximum route length. Thus in source routing protocols the energy consumption by the intermediate nodes increases by the malicious node which automatically forms the same node to appear in the route. The loop node attack strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route.

B. Long Route Attack:

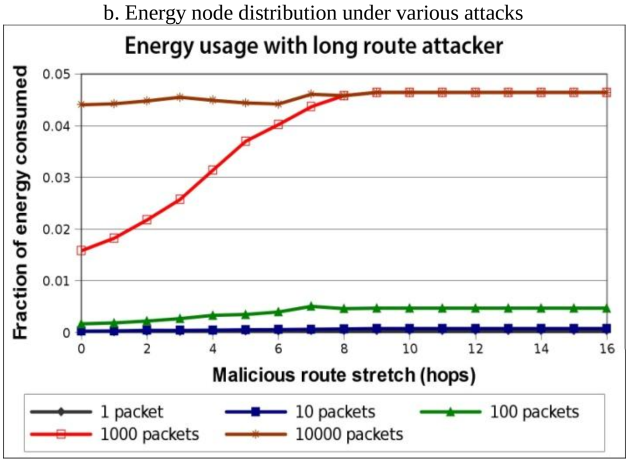
In long route attack the malicious node constructs long routes causing the packets to travel more than the original nodes. This attack also ensures the large consumption of energy to reach the destination from the source .Normally the energy will be consumed in the transmission of packets from the source to destination. This may be true in the case of honest path. But with long route attack the amount of energy consumed will be increased as the number of nodes to reach the destination increases. The malicious node causes the route to be a long with number of nodes selected. The increase in the energy usage is determined by a factor of O ((min(S, d)) where S is the number of nodes in the network and d is the maximum path length allowed. The amount of damage experienced in this attack is less than the loop node attack. Here the number of hops that to be traversed by a packet is bounded by the network nodes. The damage caused to the packet will be slightly less than the loop node attack.

Both the long route attack and loop node attack, they are causing damage only in the neighbourbood networks whereas in hierarchical networks it is less effective. A single malicious node would cause the entire network to disable if it present in the neighbourhood manner.

The Fig.b shows the attack scenarios with various attacks. The energy consumed by each attack is depicted in the below figure. With respective to the number of nodes the energy consumed by various attacks is shown. The energy consumed by the honest route is depicted with the number of nodes used. The energy consumption with long route attack is more than the honest route. In case of loop node attack, since the same node appears in the node again and again the amount of energy consumed is more than the honest route and the long route attack.



b. Energy node distribution under various attacks



c. Malicious node transmitting messages with long paths

The above fig.c shows that the energy usage consumed by the long route attack is drastically high with the number of hops used in the network .Since it enlarges the route than the honest route the energy consumption will be automatically high.The energy consumption with increase in the number of packets is depicted in the figure.The malicious route stretch formed by the node increases the energy consumption automatically.

IV.ATTACKS MITIGATION

The attacks on source routing protocols can be mitigated as follows. The loop node attack can be prevented by ensuring whether the forwarding nodes check the entire source routes for loops. This would be helpful in the malicious node environment where the node causes the same node to appear again and again in the transmission. When a loop is detected the source can correct the path in which the packet is to be transmitted .The loop node attack can also be mitigated by using a back propagating technique from the destination. In this technique each node must locate the next hop to transfer the message .If each node locate itself from the destination side the same node appears in the route can be truncated.

The long route attack is somewhat challenging than the loop node attack. The intermediate nodes must check for optimality of the route when the packet is traversed. If the in between nodes follow the same route what specified in the header then the long route is easy to proceed. Each sub node in the transmission must check for a better route by which they can reach the destination .If better route is available that route can be replaced in the header. Another way of mitigating this attack is minimizing the route length based on the expected maximum path length. Thus when the number of path length is increased than the expected maximum route length then the malicious interaction can be identified. This may not be suitable in the case of larger network where the number of nodes may be higher & may not be limited. Moreover in wireless environment rating the number of route length may affect the performance when it is extended to a larger extend.

TABLE I
DIFFERENT TYPES OF ATTACKS

Sl.N	Attacks analysis in WASN		
	Attacks	Effects	Mitigation
1	Loop node Attack	Causes the same node to appear again and again in the route	Forwarding nodes can check for loops. Can use back propagation technique from the destination side.
2	Long route Attack	Causes the larger route from source to destination than the honest route	Forwarding nodes can check for the optimality of the route.
3	Vampire Attack	Depletes the battery power consumed by each node in the network.	Vampire Algorithm

V.ATTACKS ON INTERNODE ROUTING PROTOCOLS

In internode routing protocols the network nodes aware of the network topology and its state and make the forwarding decisions based on the stored state of the node. The route discovery is done in most of the protocols by flooding the packet through the neighbourhood nodes. In some case the route discovery may be done dynamically by the nodes to chose the optimal path. Protocols such as AODV may use the nodes to find the topology at any time irrespective of the change in topology .In such cases a attack which is hard to identify and not specific to any protocol is the vampire attack.

A.Vampire attack:

In vampire attack the battery power of the nodes is drained by the malicious node.The packets to that nodes will be dropped automatically since it loses its power to send and receive the packets.Normally any type of protocol used in the wireless adhoc sensor network environment it may be involve two phases:i)Topology discovery and ii)Packet forwarding.Topology discovery includes finding the appropriate nodes in the network for transmission.It may be through broadcasting or through the flooding.In Packet forwarding the decision to forward the packet entirely depends upon the node.When receiving a packet the node determines what to do with the packet whether to receive the packet or to send the packet.The next hopto transfer the packet is identified immediately by the node.Here the routing decision is not made by the source initially whereas the intermediate nodes makes the possible route to make the packets to transfer.When one of the nodes involved in the transmission tends to be a malicious node then the battery power of the nodes goes to the dead end.Therefore the packets that reach the node my either drop or transfer to the next hop.

B.Algorithm:

The detection of the vampire attack is detected from the table maintained after the start of transmission that contains the metric number and energy level for the node. Thus, the detection can be easily carried out by matching the average energy level obtained from the node receiving the data with the abnormal energy level. If the vampire node energy level greater than the overall energy level of the nodes then the detected node is vampire. Thus, in general the algorithm for finding the vampire attack can be defined as follows:

1. While transmission=complete loop.
2. Maintain table for path selected on start of transmission containing sequence number of node.
3. Send data to relaying node.
4. Calculate the energy level of node and store the energy level of node.
5. Look for abnormal energy level received in the routing table.

6. If abnormal energy level of node is found then , the node is vampire, it is eliminated.
7. Else node is authorized.
8. End of step one loop.
9. Exit.

The above algorithm helps in efficient detection of vampire attack nodes through the energy level. First, the complete loop of the structure is assigned to the transmission. Second step a table should be maintained for each path that is selected for the transmission. Each node contains the sequence number which is already implemented using the AODV protocol. Once the nodes are identified for transmission then the data are transmitted from the source to the destination. If the destined suffers from vampire attack the entire drained from it. The packets reaching the destination would result in the drop of it. As a third step send data to the relying node. The next step is to calculate the energy level of each node and store in a routing table. The routing table denotes the entire energy level of the nodes. If the level of energy is abnormal in the routing table then the node is determined as vampire node. Such abnormal nodes are then eliminated from the structure. If the energy levels in each node is normal then they are termed as authorized. The authorized nodes will still be the part of the structure to receive packets. This algorithm confirms about the nodes whether it is attacked. This provides the efficient mechanism in identifying the nodes about their status. If there is a identification of low energy node in the transmission, then the path is traced back to find the next appropriate node. The above approach may be useful in secure transmission by finding alternate paths over the structure. But detecting such nodes in an predefined manner is not possible in an effective manner. The proposed coupon algorithm helps in detecting the vampire nodes in an efficient way.

VI.CONCLUSION & FUTURE WORK:

In this paper, various number of possible attacks in wireless ad hoc sensor networks were described. The vampire attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. We showed a graphical demonstration of varius attacks used in source routing protocols and inter node routing protocols. The proposed algorithm helps in identifing the malicious nodes that darin the battery life of particular node and retransmit the packet in sutiable path.The possible mitigation methods also analysed in that concern. Normally the vampire attack is hard to identify since it is not protocol specific. But the vampire algorithm would help in the efficient identification of tghe malicious nodes that causes the attack and eliminate it from the network.This paper can be used as an research piece in which effective methods to prevent vampire attack can be proposed in future.

REFERENCES

[1]“The Network Simulator-ns-2,” http://www.isi.edu/nsnam/ns,2012

[2] I. Aad, J.-P. Hubaux, and E.W. Knightly, “Denial of ServiceResilience 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 Software Speed Records,” Proc. Ninth Int’l Conf. Cryptology, 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 in India: Progress in Cryptology (INDOCRYPT), 2008.

[7] D.J. Bernstein, “Syn Cookies,” http://cr.yp.to/syncookies.html,1996.

[8] I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ. , 1999.

[9] J.W. Bos, D.A. Osvik, and D. Stefan, “Fast Implementations of AES on Various Platforms,” Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[10] H. Chan and A. Perrig, “Security and Privacy in SensorNetworks,” Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

BIOGRAPHIES

S.Kannan received his B.E degree in Computer Science and Engineering from Anna University, Chennai in 2010. He is currently doing M.E in Computer science and Engineering at Anna university.

A.Palanisamy received his B.E. in Computer Science and Engineering from MK University in 2003 and ME in Computer Science and Engineering from Anna University in 2011. He is a member of MISTE. He has presented papers in International and National Conferences. His research interest includes Network Security.