Energy Sucker Identifier and Energy Maximization in Wireless Networks

Kirthika.K[1], Mr.B.Loganathan[2]

1. M.Phil., Research Scholar, Department of Computer Science ,GAC , Coimbatore.
2. Associate Professor, Department of Computer Science ,GAC , Coimbatore.

Abstract: In recent trend wireless networks place a vital role and tends to different security threat. The proposal considers a new class of resource consumption attacks which is defined as Vampire attacks, not clearly defined earlier in routing protocols. The existing system used rate limiting and revocation methods to prevent energy draining issues. But those solutions failed to find the exact solution for the vampire attacks. The proposed network routing protocol provably prevents data from Vampire attacks by verifying packets consistently and makes progress toward their destinations with the verification and forwarding scheme. It proposes a new scheme named as **"eSI_eMAX (energy Sucker Identifier_ energy Maximization)"** with some perception about energy limitations due to damage. This technique tries to prevent the data from attacks and retransmits on the best optimal path. The proposed technique overcomes the data from damage and this uses optimal routing techniques and dynamic topology changes. The result show that the proposed scheme provides a best solution for both vampire and cripple attacks in wireless sensor networks.

Keywords: eSI, eMAX, Wireless Networks, optimal routing, dynamic topology.

I. INTRODUCTION

Wireless sensor networks (WSN) have become an important area of research in recent years. Due to the enormous potential of sensor networks to enable applications that connect the physical world to the virtual world, it is considered as more powerful. By setting up huge numbers of tiny sensor nodes, it is possible to obtain data about physical phenomena that was difficult or impossible to obtain in more conventional ways.

A wireless ad hoc network is referred as the collection of wireless nodes. The wireless ad hoc network can communicate directly over a common wireless channel. The nodes are equipped with wireless transceiver. Those nodes don't need any additional infrastructure, such as base station or wired access point, etc. Therefore, each node doesn't only plays the role of an end system, but also acts as a router, that sends packets to desired nodes.

Depending on the network structure the routing in wireless networks are separated into three types which are flat based routing hierarchical-based routing and location based routing. The flat-based routing performs the scheduling to all nodes are typically assigned with equal roles and functionality. The hierarchical based routing insists the nodes to play different roles in the network. The location based routing performs tracking process of the sensor nodes' positions and exploited to route data in the network effectively.

Due to the mobility and dynamic nature the wireless environment has undergo with huge set of attacks, such as QOS attacks, DOS attacks, routing attacks and Sybil attacks etc., in the recent scenario the wireless network suffers from energy based

QOS attacks, which cannot be identified by the controller easily. These kind of attacks were considered as the network problem.

In order to deal the above problem the study proposed a new proactive and reactive method named as “eSI_eMAX” which identifies the DOS, energy based attacks and enables the energy boost-up process when there is limited energy. This also uses optimal routing techniques and dynamic topology changes maintenance for accurate attack detection.

II .RELATED WORKS

Due to the on demand organization and mobility, the wireless networks are particularly vulnerable to denial of service (DoS) attacks [1].

The paper [2] addresses a special form of damage is known as PDoS (Path based Denial of Service).

In PDos attack, an adversary makes flooding attack by spreading forged packets or injected packets over multihop end to end communication path; this will engulfs the sensor node a long distance away from the other nodes. The PDos scheme used one way hash chain mechanism to prevent the end-to-end communication and flooding attacks in wireless sensor networks. The main drawback in the PDoS is, that suffers from a processing overhead, where the burden passed on the sender, who must know prior information about each node in the path in order to send the relevant verification information.

Statistical en-route filtering technique used to control attacks on compromised sensor nodes, where a compromised node can easily inject wrong report in the network. This causes exhaustion of finite resources at sensor nodes as well as causes false alarms [6]. The Statistical En-Route Filtering technique is able to detect and destroy such false reports in the network by performing the filtering policies. In order to perform the filtering process, the message authentication code (MAC) is used. This also verifies the validity of the each packet and node.

Existing Vampire attacks [5] are not a protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols. However this is not protocol specific, this exploits general properties of protocol classes such as link-state, distance vector, source routing and geographic and beacon routing. These attacks rely on flooding the network with large amounts of data. But these systems try to transmit as little data as possible to achieve the largest energy drain; this has been prevented using rate limiting solutions. Since Vampires use protocol-compliant messages. These attacks are very difficult to detect and prevent in wireless networks.

The paper [5] do not imply that power draining itself is story but rather that these attacks have not been completely defined, measure, or mitigated at the routing layer. In literature the power exhaustion can be found in [7], this has considered as “sleep deprivation torture.” As per the name, the [7] sleep deprivation torture attack prevents nodes from entering a low-power sleep cycle, and thus drains their batteries faster.

Research based on “denial of sleep” has been proposed in [8], the problem of that research is, that only considers attacks at the MAC layer. In addition some work extended at the transport layers [9] this offers the resource limitation by applying rate limitation and this could eliminate only the insider adversaries.

Malicious cycles have been briefly mentioned in [10]. However no effective defenses are discussed other than increasing efficiency of the underlying MAC. This improves the routing protocols performance by route navigation. Several power constraints existing system suffered from the QOS problems.

III.EXISTING OF PLGP AND PLGPa IN VAMPIRE ATTACKS

Existing work on protected routing attempts to guarantee that adversaries cannot cause path discovery to return an invalid network path. Even though the invalid path selection is restricted, Vampires use existing valid paths for attack.

The vampires do not disrupt or alter discovered paths but it uses exiting protocol compliant messages. The existing Protocols that maximizes power efficiency, but the protocols based on cooperative node behavior, due to this reason those cannot optimize the malicious action in wireless environment. In general the vampire attacks has been divided into two types one is carousel attacks, which targets the source routing protocols by exploiting the limited verification on message headers at forwarding nodes, this retransmits the packets in the existing nodes. The next type of attack is stretch attacks; it artificially constructs long stretched routes and potentially traverses on every node in the network. The existing system has several drawbacks such as Power Outages due to environmental disasters, information loss etc.

IV.PROBLEM DEFINITION

Vampire attacks, which is a new class of resource consumption and QOS attacks that use routing protocols to permanently disable ad hoc and wireless sensor networks by draining nodes' battery power and resources. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. Identifying and mitigating the QOS based energy draining attacks is much more important in the wireless environment. The proposed routing protocol are provably limits damage from those QOS and vampire attacks by verifying that packets consistently make progress toward their destinations and reduces the damages.

V. BEST RESULT USING ENERGY SUCKER IDENTIFIER_ENERGY MAXIMIZATION

This predicts the vampire attacks based on the existing behavior and finds optimal path and optimal topology discovery. This makes the Schedules for the energy consumption and calculates the need of energy. If any node performs vampire the system identifies the node and informs to the sender. Data transmission is based on Topology verification in the proposed system which is based on the shortest-path computation method

- In the network each node maintains a view of the network topology with a on demand cost for each link for the selected data.
- Each node will periodically broadcast the link costs, path details to its outgoing links to all other nodes via the protocol.

A. Energy and Path aware Routing protocol (EPR): This provides real-time end-to-end guarantees in WSN. The protocol requires each node to maintain routing information about its neighbors and uses geographic and attack aware forwarding to find the best paths. Estimate the end-to-end delay and energy for the packets. Moreover, EPR can provide energy when the network is compromised.

The system performs the hop by hop verification to prevent energy drain attacks. The information exchange mechanism collects information about the nodes and their energy and distances. Delay will be calculated at each node, which is basically calculating by the elapsed time after an

ACK is received from a neighbor as a response for a transmitted packet. With the consideration of the delay values, the proposed routing protocol selects the node, which meets the exact distance and energy constraint.

The EPR proposed a solution is to how intermediate nodes process the source route verification to thwart the adversaries. This performs the message verification before forwarding; after that the node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward instead from the source forward, it identifies the node as adversary, this also searches for any loop that includes the current node will be automatically truncated (the last instance of the local node will be found in the source route rather than the first). The carousel attack problem which is solved by these proposed EPR and ABT. S->A->…E->…A->…-> E->D Before E loops back it checks Path in reverse, and sends to next node accordingly-> prevents Looping, sends to D on next hop. The protocol performs the following processes.

- Every node preserves routing information for all known destinations in the network.
- The routing information should be revised occasionally.
- Traffic overhead should be calculated even if there is no change in network topology.
- The protocol insists each node to maintain the list of paths or routes and the unused route information's in the network.

B. Anti Back Tracking method (ABT): This method make sure that the data does not comes back to previous node for transmitting the data which results in energy lose. This approach incorporates the solution against energy based attacks and data security with EPR routing Protocol and ABT. This protocol provides a secure and guaranteed transmission of data. The entire process of energy sucker identifier and energy maximize involves the following steps

(1) Initialize every node

(2) Register and active a node n1, n2…Nn.
(3) Initial energy analysis
(4) Source generates data = send(source, destination, path , attestation, ABT id) where ABT is anti back tracking id which is a temporary id
(5) For each node , (EPR- message)
Send EPR(sender, receiver, seqno, abt id)
Analyze the node by their energy and distance
(6) if (Node seq no == largest seq no)
Verify routing table.
(7)Sender transmits to the verified forwarder node
(8) Apply anti backtracking method
(9) Evaluate energy
(10) If energy is sufficient then forward else perform energy maximization algorithm
(11)Monitor the node behavior and elect best forwarder
(12) Report and update the routing table.

To accomplish secured communication anonymous key is generated. To obtain reliable transmission routing scheme is used. In this approach the id for data packets and are randomly generated and the adversary cannot be able to differentiate the path details with the data packets.

C. Implementation Process:

- Node creation
- Protocol Implementation

- Results

Network Deployment:

The proposed protocol EPR performed with initial network construction process. The collection of nodes and parameters are initially constructed for experiment.

Protocol Implementation:

The system proposed a new proactive and reactive based routing protocol, which provides more reliable and effective route discovery process along with energy maximization. The protocol performs the energy sucker identification process by validating every packets and routes in the network, and predicts the resource needed by a wireless node and performs the energy maximization for further data transmission.

Simulation results:

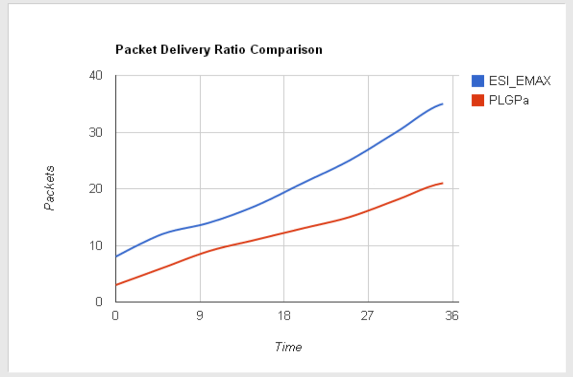
Through the effective implementation platform, the system has been implemented the EPR and ABT. The final output through the Network tool has been verified. The first step to use the trace files which is to produce the graph and final report.

The trace file contains the topology information such as list of nodes, set of links, and the packet history. As a result, internally reads information from a file and keeps only a of animation event information in memory. Its animation event has a fairly simple and consistent structure so that it can many different visualization situations.

VI. RESULT: This section deals with the performance comparison of the systems such as PLGP, PLGPa, and ESI_EMAX for vampire attack, detection and prevention.

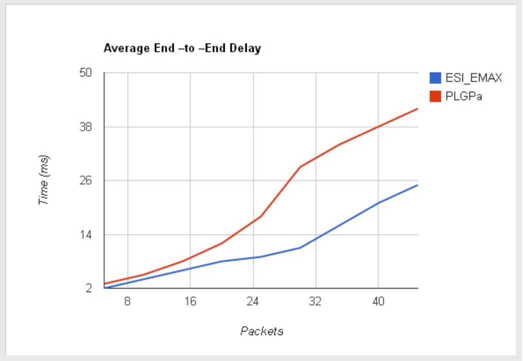
A. Packet Delivery Ratio:

The proposed protocol improves the Packet Delivery Ratio. Due to the proactive nature the Packet delivery ratio will be improved, this reduces the packet loss due to the energy drain and QOS based attacks. In general the PDR is a ratio between the received packets at the destination and the total number of packets transmitted from the source. When the packet delivery ratio is high then the performance is also high.



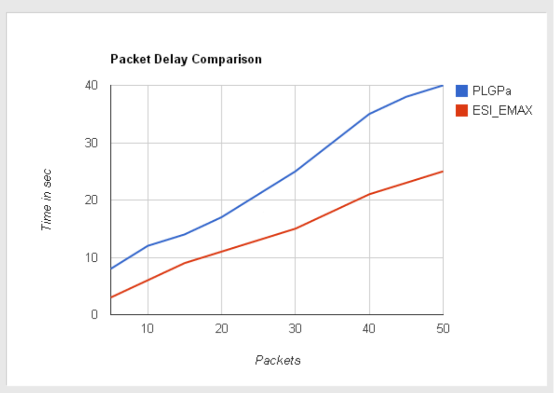
B. Average End –to –End Delay:

End to end delay is the difference between the packet receiving time and the packet sending time. Average delay is the ratio between the time difference and the total number of packets received at the destination. the average end –to –end delay shows the performance of the proposed work decreases the data delay.



C. Time Complexity:

The time complexity of an algorithm is measured as the time taken to execute a method or function by an algorithm for the given input. The time complexity of an algorithm is generally articulated using "big O" notation. Here the time complexity of ESI_EMAX is O (N) where the complexity is O (N) + 4.



VII.CONCLUSION

The paper system has implemented a energy analyzer algorithm in wireless network with the aim of detecting vampire attacks. This tend to outlined vampire attacks, a replacement category of resource consumption attacks that use routing protocols to permanently disable wireless device networks. These attacks don't depend on explicit protocols or implementations but rather expose vulnerabilities in a very variety of standard protocol categories in the network. The protocol tend to showed variety of energy based attacks against representative back tracking of existing routing protocols employing a tiny variety of weak adversaries and measured their attack success on a indiscriminately generated topology of thirty nodes. The implementation shows that the effective routing with the consideration of link stability as well as path misbehaves and vampire attack identification using the anti back tracking from every node. The paper provides two advantages one is it maintains attack free data transmission and energy boost up and another one is protection against energy drain and QOS based attack.

REFERENCES

[1]Wood A.D and Stankovic J.A, “Denial of Service in Sensor Networks,” Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

[2] Deng, Jing, Richard Han, and Shivakant Mishra. "Defending against path-based DoS attacks in wireless sensor networks." *Proceedings of the 3rd ACM workshop on Security of ad hoc and sensor networks*. ACM, 2005.

[3] Perrig, Adrian, et al. "SPINS: Security protocols for sensor networks." *Wireless networks* 8.5 (2002): 521-534.

[4] Z. Karakehayov, Using REWARD, to Detect Team Balckhole Attacks in Wireless sensor Networks Workshop on Real world Wireless Sensor Networks, (REAL WSN, 05) Stockholm, Swedan, June 2005.

[5] Vasserman, Eugene Y., and Nicholas Hopper. "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks." *Mobile Computing, IEEE Transactions on* 12.2 (2013): 318-332.

[6] Fan. Ye, H. Luo, Songwu. Lu. L. Zhang. Statistical en-route Filtering of injected False Data in Sensor Networks IEEE Journal on Selected Areas in Communications, Vol-23, (4), pp. 839-850, April 2005.

[7] F. Stajano and R. Anderson, “The Resurrecting Duckling: Security Issues for Ad-Hoc Wireless Networks” Proc. Int’l Workshop Security Protocols, 1999.

[8] D.R. Raymond, R.C. Marchany, M.I. Brownfield, and S.F. Midkiff “Effects of Denial-of-Sleep Attacks on Wireless Sensor Network MAC Protocols” IEEE Trans. Vehicular Technology, vol. 58, no. 1, pp. 367-380, Jan. 2009.

[9] D.R. Raymond and S.F. Midkiff, “Denial-of-Service in Wireless Sensor Networks: Attacks and Defenses” IEEE Pervasive Computing, vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.

[10] B. Parno, M. Luk, E. Gaustad, and A. Perrig, “Secure Sensor Network Routing: A Clean-Slate Approach,” CoNEXT: Proc. ACM CoNEXT Conf., 2006.