IJISET - International Journal of Innovative Science, Engineering & Technology, Vol. 1 Issue 3, May 2014.
www.ijiset.com

ISSN 2348 – 7968

Detection of Vampre Attack Using EWMA in Wireless Ad Hoc Sensor Networks

S.Manimala[1], A.Taskala Devapriya[2]

[1]. PG Scholar, Communication Systems, Mount Zion College of Engineering and technology,
Pudukkottai - 622507,Tamil Nadu, India

[2]Assistant Professor, Department of Electronics and Communication Engineering
Mount Zion College of Engineering and technology, Pudukkottai-622507, Tamil Nadu, India

ABSTRACT- Ad-hoc sensor network and routing data in them is a significant research area. There are a lot of protocols developed to protect from DOS attack, but it is not completely possible. One such DOS attack is Vampire attack-Draining of node life from wireless ad-hoc sensor networks. In this project, presents a method to tolerate the attack by using the EWMA method. In case this, any Vampire attack, the EWMA method engages in the situation and delivers the packet to destination without dropping the packet. Thus providing a maximum lifetime of the battery and reliable message delivery even in case of Vampire attack.

Index terms: Ad hoc sensor network, Energy consumption, Routing , Security, DOS.

I.INTRODUCTION

Wireless sensor Network (WSN) consists of mostly tiny, resource-constraint, simple sensor nodes, which communicate wirelessly and form ad hoc networks in order to perform some specific operation. Due to distributed nature of these networks and their deployment in remote areas, these networks are vulnerable to numerous security threats that can adversely affect their proper functioning. Simplicity in WSN with resource constrained nodes makes them very much vulnerable to variety of attacks. The attackers can eavesdrop on its communication channel, inject bits in the channel, replay previously stored packets and much more. The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power. The communications links available for coordinating their attack. The sensor nodes may not be tamper resistant and if an adversary compromises a node, it can extract all key material, data, and code stored on that node. As a result, WSN has to face multiple threats that may easily hinder its functionality and nullify the benefits of using its services.

An adversary can easily retrieve valuable data from the transmitted packet that are sent (Eavesdropping). That adversary can also simply intercept and modify the packets content meant for the base station or intermediate nodes (Message Modification), or retransmit the contents of those packets at a later time (Message Replay). Finally, the attacker can send out false data into the network, maybe masquerading as one of the sensors, with the objectives of corrupting the collected sensors reading or disrupting the internal control data (Message Injection). Securing the WSN needs to make the network support all security properties: confidentiality, integrity, authenticity and availability.

Attackers may deploy a few malicious nodes with similar or more hardware capabilities as the legitimate nodes that might collude to attack the system cooperatively. The attacker may come upon these malicious nodes by purchasing them separately, or by "turning" a few legitimate nodes by capturing them and physically overwriting their memory. Also, in some cases colluding nodes might have high-quality communications links available for coordinating their attack. The sensor nodes may not be tamper resistant and if an adversary compromises a node, it can extract all key material, data, and code stored on that node. As a result, WSN has to face multiple threats that may easily hinder its functionality and nullify the benefits of using its services.

Routing and data forwarding is a crucial service for enabling communication in sensor networks. Unfortunately, current routing protocols suffer from many security vulnerabilities. For example, an attacker might launch denial of-service attacks on the routing protocol, preventing communication. The simplest attacks involve injecting malicious routing information into the network, resulting in routing inconsistencies. Simple authentication might guard against injection attacks, but some routing protocols are susceptible to replay by the attacker of legitimate routing messages. The wireless medium is inherently less secure because its broadcast nature makes eavesdropping simple. Any transmission can easily be intercepted, altered, or replayed by an adversary. The wireless medium allows an attacker to easily intercept valid packets and easily inject malicious ones. Although this problem is not unique to sensor networks, traditional solutions must be adapted to efficiently execute on sensor networks.

II.OVERVIEW

The extreme resource limitations of sensor devices pose considerable challenges to resource-hungry security mechanisms. The hardware constraints necessitate extremely efficient security algorithms in terms of bandwidth, computational complexity, and memory. This is no trivial task. Energy is the most precious resource for sensor networks. Communication is especially expensive in terms of power.

Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life. This attack is not specific to any protocol. Few kinds of attacks are carousal and stretch attack.

CAOUSEL ATTACK

An adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles. It is also called carousel attack. It targets source routing protocols by exploiting the limited verification of message headers at forwarding nodes, allowing a single packet to repeatedly traverse the same set of nodes. This 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. The thick path shows the honest path and thin shows the malicious path.

STRETCH ATTACK

An adversary causes packet to travel long distance than the needed to reach the destination leading to energy wastage. Thus both lead to consumption of energy unnecessary. The honest path is very less distant but the malicious path is very long to make more energy consumption. Per-node energy usage under both attacks.The stretch attack shows more uniform energy consumption for all nodes in the network, since it lengthens the route, causing more nodes to process the packet. While both attacks significantly network-wide energy usage, individual nodes are also noticeably affected, with some losing almost 10 percent of their total energy reserve per message. It increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination.

III.RELATED ATTACKS

Jelly Fish Attack: This type of attack is used for closed loop flow such as TCP. A critical strength of the Jelly Fish Attack is that it maintains compliance with all control plane and data plane protocols in order to make detection and diagnosis costly and time consuming. The key principle that Jelly Fish attack use to facilitate is targeting end-to end congestion control. Black Hole Attack: This type of attack is used for open loop control flows. Black Hole nodes participate in all routing control plane operations. However, once paths are established, Black Holes simply drop all packets. Although refusing to forward data is not protocol compliant.

IV.ENERGY WEIGHTED MONITORING ALGORITHM

The details of our proposed protocol EWMA. Where energy of a node gets to threshold level it plays a vital role by performing energy intensive tasks there by bringing out the energy efficiency of the sensors and rendering the network endurable. This pattern based on the energy levels of the sensors.

EWMA functions two phases namely.

1. Network configuring phase

2. Communication phase

NETWORK CONFIGURING PHASE*:* The goal of this phase is to establish a optimal routing path from source to destination in the network. The key factors considered are balancing the load of the nodes and minimization of energy consumption for data communication.

Now the node establishes the routing path, first the traces the next node by computing the energy required to transmit the required data packet that is suitable energy node and less distant node selected as the next forwarding node in this way it establishes the route from source to destination with suitable energy and less distant. Thus energy spent by the allotted node suitable to the data packet sent from the node in this way this algorithm avoids data packet dropping and this allotted forwarding node transmits the packets safely to the destination. This algorithm gives prime importance to achieve balancing of load in the network. The suitable energy node will be assigned as a forwarding node as long as this node as this node has the capacity to handle. In this way a multi hop minimal less distant path is established to bound the network damage from vampire attack.
EWMA avoids the collapsing of entire network by dropping the packets in the network. The load is evenly balanced depending upon the capacity of the nodes. In this way multi hop load balanced network is achieved.

FLOW CHART:

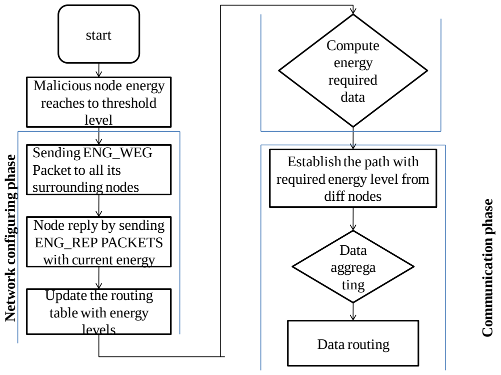
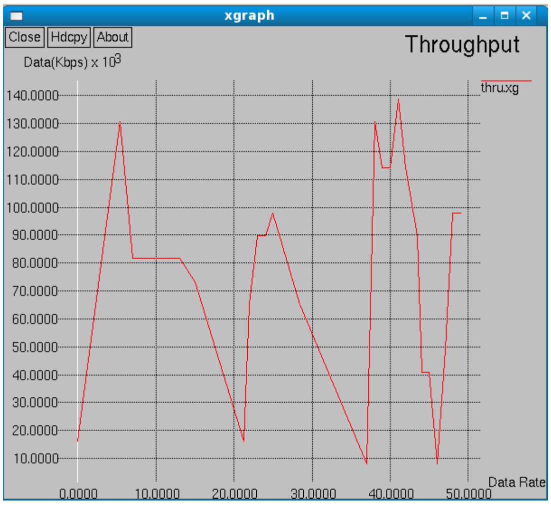
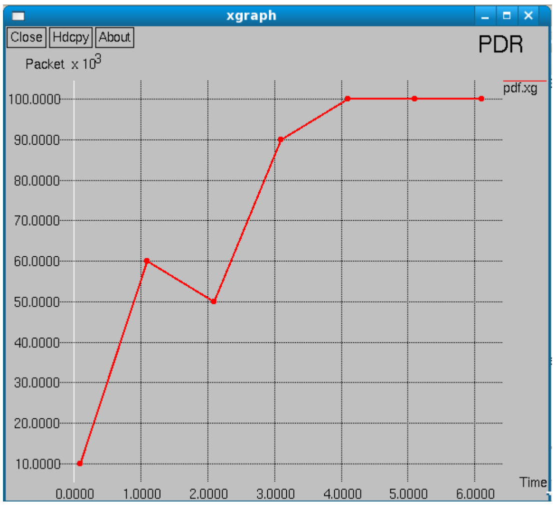

start
Malicious node energy reaches to threshold level
Sending ENG_WEG Packet to all its surrounding nodes
Node reply by sending ENG_REP PACKETS with current energy
Update the routing table with energy levels
Network configuring phase
Compute energy required data
Establish the path with required energy level from diff nodes
Data aggrega ting
Data routing
Communication phase

Figure4.1 Flow Chart of EWMA in wireless sensor.





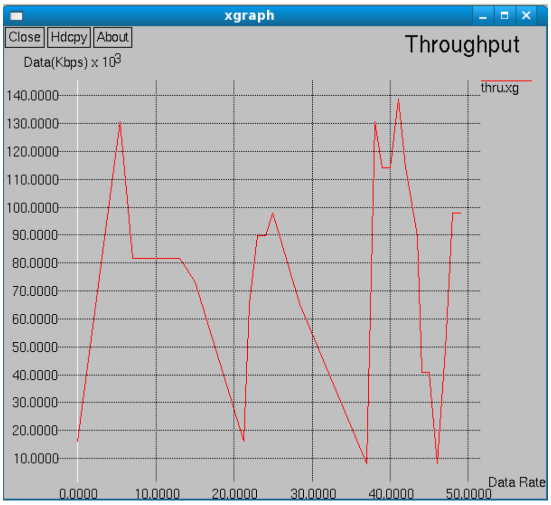


Figure 4.2Throughput Vs data rate

V.TOPOLOGY DISCOVERY

Discovery begins with a time limited period during which every node must announce its presence by broadcasting a certificate of identity, including its public key signed by a trusted offline authority. Groups merge preferentially with the smallest neighboring group, which may be a single node. Groups that have grown large enough that some members are not within radio range of other groups will communicate through "gateway nodes," which are within range of both groups.

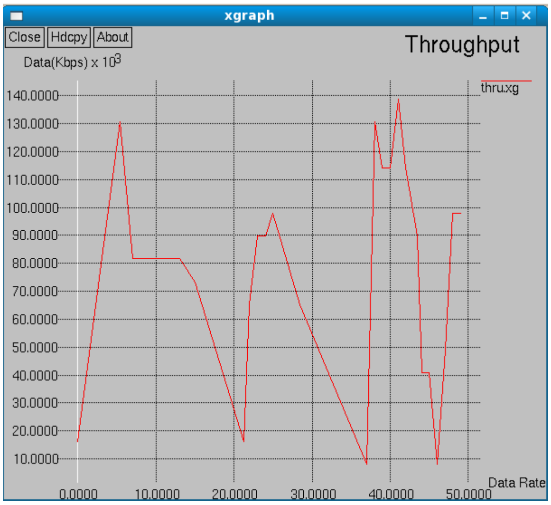


Figure4.3 PDRVs data rate

VI.PACKET FORWARDING

During the forwarding phase, all decisions are made independently by each node. When receiving a packet, a node determines the next hop by finding the most significant bit of its address that differs from the message originator's address. Thus, every forwarding event (except then a packet is moving within a group in order to reach a gateway node to proceed to the next group) shortens the logical distance to the destination, since node addresses should be strictly closer to the destination.

VII.IMPLEMENTATION

To measured their attack success on a randomly generated topology of 20 nodes. Simulation results show that depending on the location of the adversary network energy expenditure during the forwarding phase increases. All experiments were performed on Pentium IV core 2 Duo PC with 3 GB of main memory, running fedora 10. All procedures were coded in NS2.

The range of time and PDR has been taken for plotting the graph experienced by the network during the packet transmission.

VIII. CONCLUSIONS

In this paper we talk about Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad-hoc wireless sensor networks by depleting nodes' battery power. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols. We also saw how to overcome vampire attacks thus increasing the energy of the node by a factor of O(N) per adversary per packet, where N is the network size. We defined about EWMA the first sensor network routing protocol that provably bounds damage from vampire attacks by verifying the packets towards the destination. Derivation of damage bounds and defences for topology discovery, as well as handling mobile networks, is left for future work.

IX. ACKNOWLEDGMENT

We would like to thank our college Mountzion college of Engineering and Technology,our guide Mrs. A. Taksala Devapriya and other staff for their continuous support and for their helpful comments on the earlier drafts of this paper.

X.REFERENCES

[1]. Ad .I, Hubaux J.P, and E.W. Knightly. E.W, "Denial of Service Resilience in Ad Hoc Networks," Proc. ACM MobiCom, 2004.

[2]. Aces. G, Butt an .L, and Vajda .I, "Provably Secure On-Demand Source Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[3]. Bhandare .S, T.X. Brown, and S. Doshi "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.

[4]. Bryan Par no, Mark Luk, Evan Gaustad, and Adrian Per rig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006**.**

[5]. Chang.H.J and Tassiulas .L, "Maximum Lifetime Routing in Wireless Sensor Networks," IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

[6]. Daniel Bernstein and Peter Schwa be, New AES software Speed records, INDOCRYPT, 2008.

[7]. Douceur.R.John, the Sybil attack, International workshop on peer-topeer systems, 2002.

[8]. Deng.J, Han.R, and Mishra.S, "Defending against Path-Based
Attacks in Wireless Sensor Networks," Proc. ACM Workshop Security of Ad Hoc and Sensor Networks, 2005.

[9]. Eugene Y.Vasserman, Nicholas Hopper, Vampire attacks: Draining life from wireless ad-hoc sensor networks.2011

[10]. Feeney.L.M, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001.

[11]. Karloff.S and Wagner.G, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.

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

[13]. Yih-Chun Hu, Perrig Adrian, and Johnson. David B., Ariadne: A secure on-demand routing protocol for ad hoc networks, MobiCom, 2002