Detection and Prevention of Energy Draining Attack With Reduced Overhead

Mrunal Arjunkar
M.Tech.
Dept. of C.S.E. P.I.E.T.
Nagpur, India

Ashish S. Sambare
H.O.D. Dept. of C.Tech. P.I.E.T.
Nagpur, India

ABSTRACT
Survivability of network is its ability of being connected even below failures and attacks. Activity procedure of a device network at intervals the hostile setting leads it to battery drain attacks, because it isn't gettable to recharge and even replace device node's battery power. The motivation provided for the analysis efforts has been given by an inspiration maximization of network quantity, wherever the number of network is live of the moment of activity to the aim. Once any of the nodes has exhausted its restricted power provide and becomes in-operational normally referred as 1st node failure. Even a very distinctive approach for routing protocols, have an effect on from attacks those unit designed to be protected, unit unable to provide protection from these attacks, that decision vampire attacks. This might be a class of resource intense attacks that for good disable the entire network by quickly enfeebling battery of nodes. These attacks don't seem to be specific to any specific routing protocol, unit serious, powerful to look out and unit very easy to hold out victimization as few reciprocally malicious government inflicting solely protocol compliant messages throughout this novel approach, each phases of protocol unit thought of avoid attack or tolerate the attack. Here rule overhead is reduced and discovery section is taken into consideration to avoid vampire attack.

Keywords
Ad-hoc wireless sensor networks, Routing Protocols, Denial of Service attack, Energy consumption, vampire Attacks.

1. INTRODUCTION
The term wireless sensor network (WSN) is a network consisting of spatially distributed autonomous sensors. Those are accustomed monitor physical or maybe together environmental conditions. The various conditions are temperature, sound, pressure, etc. They also hand in glove pass their info through the network to a main location. The modern networks are duplex, that also enabling management of sensory activities. The design and development of wireless device networks were driven by military applications like parcel investigation. Now, these networks are utilized in several industries and shopper applications, like methodology observance and management, machine health observance, and plenty of countless. The WSN is created of "nodes" - from several of too several voluminous or perhaps thousands, where each node is connected to a minimum of one (or sometimes several) sensors. Each such device network node has typically many parts: a radio transceiver with an internal degree antenna or association to an external antenna, a micro-controller, associated qualification electronic circuit for interfacing with the sensors associate degreed AN energy supply, typically device or qualification embedded kind of energy gathering. The vampire attack is written as a result of the composition and transmission of message that causes much energy to be consumed by the network than if an honest node (unaffected node) transmitted a message of identical size to identical destination, though follow wholly totally utterly totally different packet headers. The strength of attack is typically measured by the relation of network energy used among the quality case to the energy utilized in malicious case. Among the secure and safe case of vampire attack, the relation is one. Energy consumption of malicious node isn't thought of, as they go to oftentimes drain their own batteries unilaterally.

2. CLASSIFICATION OF ATTACK
The first challenge in addressing vampire attacks is method them — what actions extremely represent associate attack? DoS [11, 12] attacks in wired networks are usually characterized by amplification [5, 4]: associate opponent can amplify the resources it spends on the attack, e.g. use one minute of its own equipment time to cause the victim to use ten minutes. However, place confidence in the strategy of routing a packet in any multi-hop network: a offer composes and transmits it to succeeding hop toward the destination, that transmits it a lot of, until the destination is reached, intense resources not alone at the availability node but to boot at every node the message moves through. If we've an inclination to place confidence in the accumulative energy of an entire network, amplification attacks are endlessly accomplishable, given that associate opponent can compose and send messages that are processed by each node on the message path. So, the act of inflicting a message is in itself associate act of amplification, leading to resource exhaustion, as long as a result of the mix price of routing a message (at the intermediate nodes) isn't up to the price to the availability to compose and transmit it. So, we've an inclination to ought to drop amplification as our definition of malice associated instead focus on the accumulative energy consumption increase that a malicious node can cause whereas inflicting identical style of messages as an honest node.

We define a vampire attack[1] as a result of the composition associated transmission of a message that causes further energy to be consumed by the network than if an honest node transmitted a message of identical size to identical destination, although practice utterly totally different packet headers. We've an inclination to measure the strength of the attack by the relation of network energy utilized within the benign case to the energy utilized within the malicious case, i.e. the relation of network-wide power utilization with malicious nodes gift to energy usage with alone honest nodes once the number and size of packets sent remains constant. Safety from vampire attacks implies that this relation is one. Energy use by malicious nodes is not thought-about, since they're going to endlessly unilaterally drain their own batteries.

3. LITERATURE SURVEY

The analysis on this subject is usually gyrated security solutions victimization stratified approach. Physical layer in conjunction with rest totally different layers named data-link, network, transport and application layer area unit the constituents of protocol stack within the stratified approach. The 3 planes (power management plane, quality plane and task management plane) in conjunction with the 5 layers forms wireless stratified vogue. So on boost the energy potency of wireless device networks, there's analysis phenomenon. Several of them are mentioned below:

3.1 Denial of Service Resilience in Ad-hoc Networks

Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly declared in [2] that necessary progress has been created towards making unplanned networks secure and DoS resilient. However, little or no attention has been focused on quantifying DoS resilience: Do unplanned networks have sufficiently redundant ways and counter-DoS mechanisms to make DoS attacks principally ineffective? Or are there attack and system factors which will lead to devastating effects? Throughout this paper, we have a tendency to tend to vogue and study DoS attacks therefore on assess the damage that difficult-to-detect attackers can cause. The primary attack we have a tendency to tend to check, called the JellyFish attack, is targeted against closed-loop flows like TCP; although protocol compliant, its devastating effects. The second is that the region attack, that has effects nearly just like the JellyFish, but on open-loop flows. We have a tendency to tend to quantify via simulations and analytical modeling the quantify-ability of DoS attacks as operate of key performance parameters like quality, system size, node density, and counter-DoS strategy. One maybe stunning result's that such DoS attacks will increase the capability of ad hoc networks, as they starve multi-hop flows and solely enable one-hop communication, a capacity-maximizing, nevertheless clearly undesirable scenario.

3.2 Defending Against Path-based DoS Attacks in Wireless Sensor Networks

Denial of service (DoS) attacks will cause serious damage in resource-constrained, wireless device networks (WSNs). This paper addresses academic degree notably damaging style of DoS attack, noted as PDoS (Path-based Denial of Service) [6]. In academic degree passing PDoS attack, academic degree soul overwhelms device nodes a drawn-out distance away by flooding a multi-hop end-to-end communication path with either replayed packets or injected spurious packets. This paper proposes a solution exploitation unidirectional hash chains to safeguard end-to-end communications in WSNs against PDoS attacks. The planned resolution is light-weight, tolerates busty packet losses, and can simply be enforced in modern WSNs. The paper presents report on performance measured from a paradigm implementation.

3.3 An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad-hoc Networks

A mobile accidental network (or manet) is additionally a cluster of mobile, wireless nodes that hand in glove kind a network freelance of any mounted infrastructure or centralized administration. Especially, a Manet has no base stations: a node communicates directly with nodes among wireless vary and indirectly with all totally different nodes employing a dynamically-computed, multi-hop route via the choice nodes of the Manet. Simulation and experimental results area unit combined to purpose that energy and information measure are substantively totally wholly totally different metrics that resource utilization in Manet routing protocols isn't utterly addressed by bandwidth-centric analysis. It presents a model for evaluating the energy consumption [8] behavior of a mobile unplanned network. The model was accustomed examine the energy consumption of 2 well-known Manet routing protocols. Energy-aware analysis of performance is shown to provide new insights into high-priced protocol behaviors and suggests opportunities for improvement at the protocol and link layers.

3.4 Maximum Lifetime Routing In Wireless Sensor Networks

This paper show that the matter of routing messages in passing terribly wireless device network therefore on maximize network amount of your time [7] is NP-hard. In our model, the web model, every message needs to be routed whereas not knowledge of future route requests. It develops along a web heuristic to maximize network amount of your time. Our heuristic, that performs 2 shortest path computations to route each message, is superior to previously written heuristics for time period maximization our heuristic winds up in larger time period and its performance may be a smaller quantity sensitive to the selection of heuristic parameters. To boot, our heuristic is superior on the flexibility metrics.

3.5 Minimum Energy Mobile Wireless Networks

As we can observe [9] describes a distributed position-based network protocol optimized for minimum energy consumption in mobile wireless networks that support peer-to-peer communications. Given any quite haphazardly deployed nodes over a district, we've AN inclination to tend as an example that an easy native improvement theme dead at each node guarantees durable property of the total network and attains the world minimum energy solution for stationary networks. Thanks to its localized nature, this proves to be self-reconfiguring and stays close to the minimum energy solution once applied to mobile networks. Simulation results are accustomed verify the performance of the protocol.

4. PROPOSED SYSTEM

The proposed work shown in figure 1 provides solution for the two problems in the existing method. In the proposed work, reduced overhead PLGP [3] based method, mainly focused on avoiding vampire attacks in the discovery phase of PLGP by checking signal strength of the nodes which transmit the group joining messages. A vampire would send high energy signal so as to suppress the group joining messages of other node. So avoid a node which sends at high signal strength. Function modification of discovery phase (node) defines this concept. Another focus is to reduce overhead of PLGPa [1] by using single encryption instead of chain of encryption.

Proposed method concept

In this novel technique the attestation method is as shown below:

1. Encrypt the message using a secret key, then the packet includes encrypted data, cost of the operation, sender's identity (A). The whole data are encrypted with private key of A then this packet send to B as in previous case.

ENC((Msg)Prk,4,A)PrA == X => B

2. When B receives the packet decrypts it and retrieves the encrypted message only. After retrieving the encrypted message B then includes the path information along with the updated cost into the packet. These whole information's are encrypted with B's private key and send to C.

B => DEC(X)PA => ENC((Msg)Prk,3,AB)PrB == Y => C

3. When C receives the packet, above process will repeat as shown below:

C => DEC(Y)PB =>ENC((Msg)Prk,2,ABC)PrC == Z => D

D => DEC(Z)PC =>ENC((Msg)Prk,1,ABCD)PrD => D

Based on these ideas Secure_forward_packet(p) can be changed or modified.

Modified_discovery_phase(node)

if(transmit_power(node)>THRESHOLD) then

return / drop (node)*/*

else

insert_into_routingtable(node)

end if

{This small modification is very easy to understand.

In this we are going to set a threshold value. This will indicate the highest Energy value.

Let, threshold T= 15J

N1(node)=10J ACCEPTED & ADDED to RT

N2(node)=17J REJECTED}

Modified_forward_packet(p)

s = extract_source_address(p)

a = extract_attestation(p)

if(not verify_source_sig(p)) or (empty(a)) and not is_neighbour(s)) then

*return /*drop(p)*/*

prevnode = node

if(not are_neighbours(node,prevnode)) or (not making_progress(prevnode,node)) then

*return /*drop(p)*/*

end if

end if

c = closest_next_node(s)

P = saowf_append(p)

if(is_neighbours(c)) then

forward(P,c)

else

forward(P,next_hop_to_non_neighbour(c))

end if

{Source address is extracted from packet 'p' in 's' here it is 0.0.0.0

Attestation is extracted from packet 'p' in 'a' here let's take a no. 443

In the 3rd step it will verify

- If not source(i.e. other than 0.0.0.0) OR
- If 'a' is null & not neighbor 's' OR
- If not verified 'a' THEN return(/*drop*/)
- Current node will be then previous one (0.0.0.1 is previous and current will be 0.0.1.0)

If not neighbor OR not progressing, THEN return(/*drop*/)

Closest next node of 's' is assigned to 'c' (if 'all is well' then c=0.0.0.1)

Old 'p' is appended key & assigned to 'P' ('p' is appended with c's key)

Forward (P, c) if they are neighbor ('P' is forwarded to neighbor 'c')

Otherwise forward(P, c) to next hop which is non neighbor}.

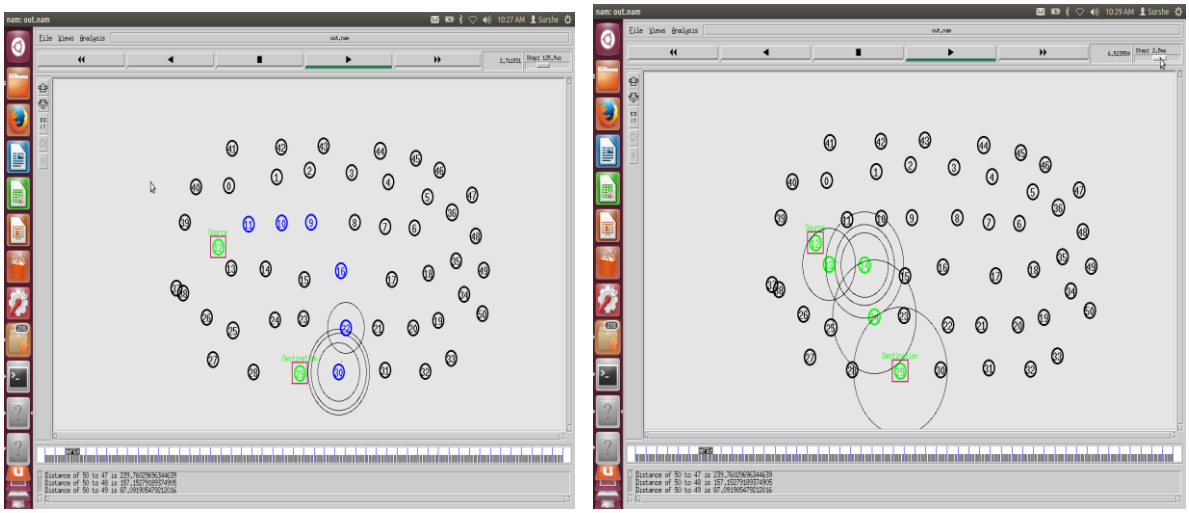

Fig 1: Snapshots of Proposed System

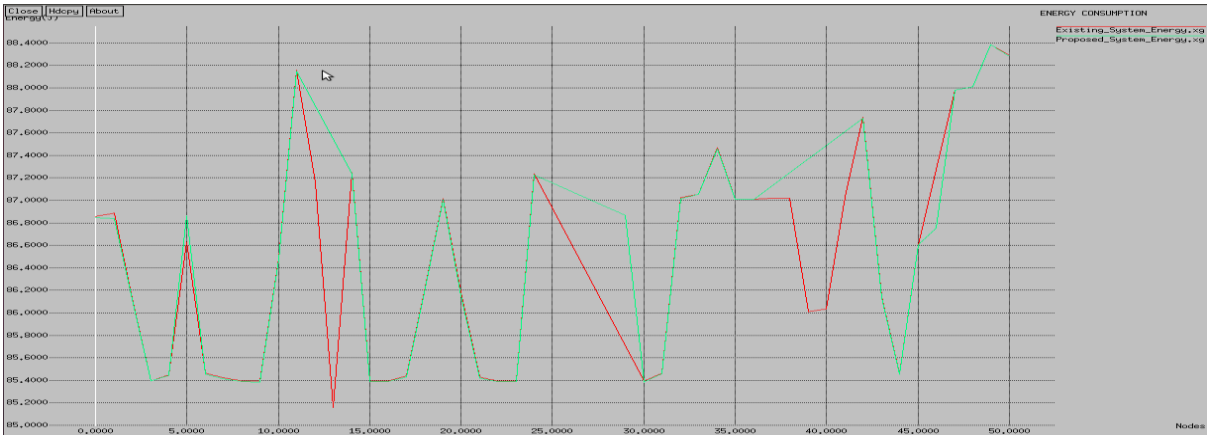

Fig 2: Energy consumed vs. Nodes

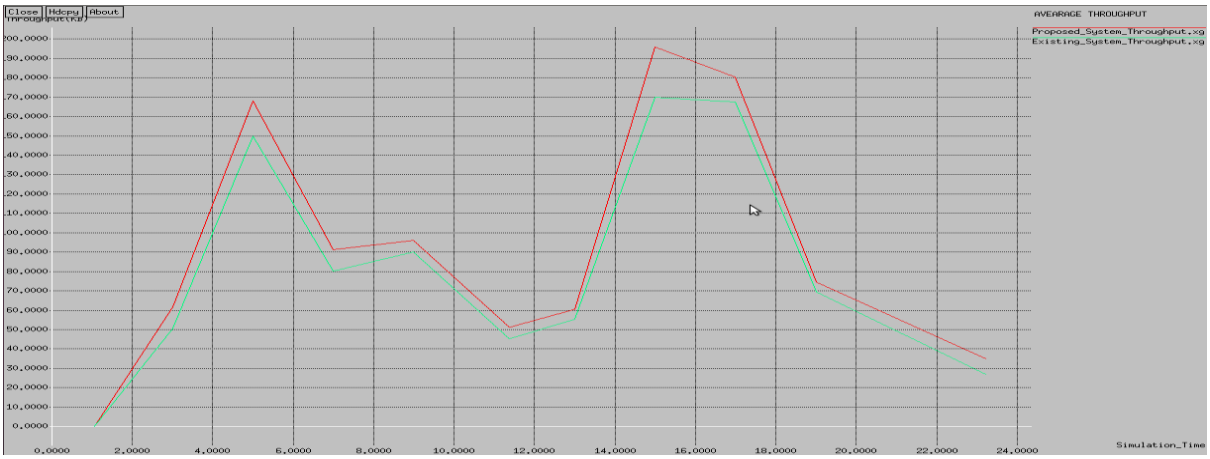

Fig 3: Average throughput vs. Simulation time

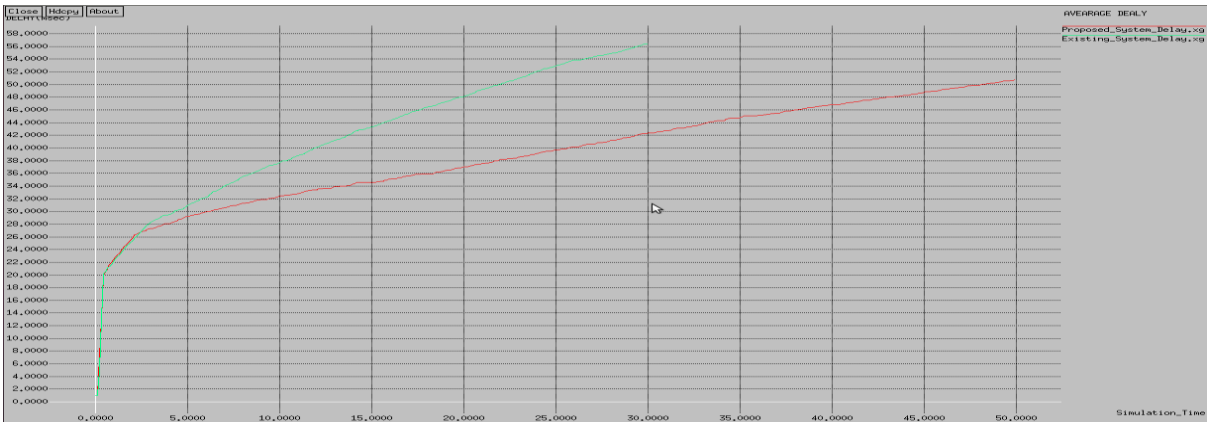

Fig 4: Average delay vs. Simulation time

5. RESULT AND COMPARATIVE ANALYSIS

Vampire attacks possess a serious threat to security of wireless sensor network. The proposed work has been compared based on various parameters. The various parameters used are energy consumption, average throughput, average delay etc.

Every node is having own energy at initial stage. Energy consumed by the nodes while forwarding packet from source to destination in existing and proposed methods are shown in figure 2.

Throughput of the whole system in the existing and proposed scenario is compared in the figure 3 graph of average throughput. We can easily identify that the throughput is increased in proposed method.

The time required to packet to travel from source to destination is reduced. Thus average delay is reduced in the proposed system if we compare it to existing one. We can notice the difference in the figure 4.

Due to the chain attestation process size of the packet in existing method is higher than proposed method. It is clear that the encryption overhead is reduced by reducing the chain attestation process to single encryption [10].

6. CONCLUSION

The Wireless sensor Network is a rising space that has wide applications. Thus the protection in wireless sensor network is of nice concern. vampire attacks are necessary attack against a wireless sensor network within which an individual develop and transmit messages that causes a lot of energy to be consumed by the network than if an honest node transmitted a message of identical size to constant destination, though mistreatment totally different packet headers. Therefore it's vital to discover the vampire nodes as early as potential. Here PLGP protocol is employed to use the vampire attacks.

Since PLGP has 2 phases evil spirit node detection is additionally exhausted this 2 phases. The novel rule is that the initial sensor network routing protocol that demonstrably bounds the harm from vampire attack in 2 phases of PLGP. This methodology reduces the energy consumption, packet overhead, cryptography efforts etc. Here solely PLGP protocol is taken into account, however the projected resolution works in alternative routing protocol isn't thought of. This methodology may be any extended to work out this downside.

7. REFERENCES

[1] Eugene Y. Vasserman, Nicholas Hopper," Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks", IEEE transactions on mobile computing, VOL. 12, NO. 2, February 2013.

[2] Imad Aad, Jean-Pierre Hubaux, and Edward W. Knightly, Denial of service resilience in ad hoc networks, MobiCom, 2004.

[3] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean-slate approach, CoNEXT, 2006.

[4] Vern Paxson, An analysis of using reflectors for distributed denial-of-service attacks, SIGCOMM Comput. Commun. Rev. 31 (2001), no. 3.

[5] Kihong Park and Heejo Lee, On the effectiveness of probabilistic packet marking for IP traceback under denial of service attack, INFOCOM, 2001.

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

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

[8] L.M. Feeney, "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.

[9] Volkan Rodoplu and Teresa H. Meng, "Minimum energy mobile wireless networks", IEEE Journal on Selected Areas in Communications 17 (1999), no. 8.

[10] Amitabh Saxena and Ben Soh, One-way signature chaining: a new paradigm for group cryptosystems, International Journal of Information and Computer Security 2 (2008), no. 3.

[11] David R. Raymond, Randy C. Marchany, Michael I. Brownfield, and Scott F. Midkiff, "Effects of denial-of-sleep attacks on wireless sensor network MAC protocols", IEEE Transactions on Vehicular Technology 58 (2009),no.1.

[12] David R. Raymond and Scott F. Midkiff, "Denial-of-service in wireless sensor networks: Attacks and defenses", IEEE Pervasive Computing 7 (2008), no. 1.