International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)

ISSN: 0976-1353 Volume 8 Issue 1 –APRIL 2014.

DETECTION OF VAMPIRE ATTACKS USING OPTIMAL ENERGY BOOST-UP PROTOCOL IN WSN's

Thanmanam. P [#1], Suguna. M[#2]

[#] *Department of Information Technology*

[*1] *PG Student, Department of Information Technology, SNS College of Technology, Coimbatore, India.*

[*2] *Associate Professor, Department of Information Technology, SNS College of Technology, Coimbatore, India.*

***Abstract*—Ad-hoc low-power wireless networks are an exciting research direction in sensing and the computing based on pervasive. In previous security work in this area have been focused mainly on denial of communication at the routing or medium access control level. The latest approach discovers resource depletion attacks at the routing protocol layer, which always restrict networks by quickly draining nodes' battery power. These "Vampire" attacks are not specific to any specific protocol, but fairly rely on the things of many popular classes of routing protocols. Finding that all examined protocols are susceptible to Vampire attacks, which are overwhelming, problematic to detect, and are relaxed to carry available using as few as one malicious insider sending only protocol compliant messages**

Keywords –**Denial of Service, security, routing, ad hoc networks, sensor networks, wireless networks.**

I. INTRODCTION

A Wireless Ad hoc Network (WSNs) is a collection of nodes which are able to connect on a wireless medium to form an arbitrary and dynamic network. Implicit herein is the characteristic of the network topology to change overtime as links in the network appear and disappear. In order to enable communication between any two nodes, a routing protocol is employed. The abstract task of the routing protocol is to discover the topology (as the network is dynamic, continuing changes to the topology) to ensure that each node is able to acquire a recent image of the network topology to construct routes.

AD hoc wireless sensor networks (WSNs) promise exciting new applications in the near forthcoming, such as abundant on-request computing power, constant connectivity, and instantly deployable communication for military and first responders. Such networks already displayenvironmentally friendlyconditions, industrial unitenactment, and troop setting out, to name a few solicitations. As Wireless sensor networks becomes more and more crucial to the everyday functioning of people and companies, availability errors become less bearable lack of availability can make the difference between businesses as usual and lost productivity, power outages, and environmental disasters. Thus high availability of these networks is a dangerous property, and should hold even under nasty conditions.

Due to their ad hoc organizations, wireless ad hoc networks are on the whole vulnerable to denial of service DoSattacks and a bigcontract of investigationhave been done to enhance survivability. These schemes can prevent attacks on the short-term availability of a network; they do not attack that affect long-term availability the most permanent denial of service attack is to entirely deplete battery nodes. This is acase of a resource running down attack, with battery control as the source of interest. Considered how protocols of routing, even those designed to be safe, lack of defences from these attacks, which called as Vampire attacks, since they drain the power of the battery life from networks nodes.

These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but relatively work extra time to totallyrestrict a network. While some of the separate attacks are simple, and draining the power and resource energy attacks have been discussed before prior work has been mostly confined to other levels of the protocol stack, e.g., medium access control (MAC) or application layers, and to the knowledge there is little discussion, and no thorough analysis, mitigation, or routing-layer resource exhaustion attacks.

Vampire attacks are not protocol-specific, in that they don't depend on properties of design or implementation faults of particular protocols of routing, but rather daring act general things of protocol classes such as link-state, space vector, routing of source and physical and ideal routing. Neither do these attacks depend on spilling over the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest draining of energy, checkinganamount limiting solution. Since the Vampires use protocol-compliant messages, these attacks are very problematic to find and prevent.

II. RELATED WORK

Denial of service (DoS) attacks can cause serious damage in resource constrained, wireless sensor networks (WSNs). This paper addresses an especially damaging form of DoS attack, called PDoS.In a PDoS attack, an opponentoverpowers sensor nodes a long distance away by flooding a multi hop end-to-end communication path with either replayed packets or injected false packets. This paper suggests a solution using one-technique hash chains to protect end-to-end communications in WSNs against PDoS attacks. The suggested solution is serious;put up withbursty packet wounded, and can easily be executed in recent WSNs. This paper information on performance measured from a prototype implementation [2].

A minimum energy routing protocol reduces the energy consumption of the nodes in a wireless ad hoc network by routing packets on routes that consume the minimum amount of energy to get the packets to their destination. This paper identifies the necessary features of an on-demand minimum energy routing protocol and suggests mechanisms for their implementation. Highlighted the importance of efficient caching techniques to store the minimum energy route information and propose the use of an ’energy aware’ link cache for storing this information. Comparing the performance of an on-demand minimum energy routing protocol in terms of energy savings with an existing on-demand ad hoc routing protocol via simulation. Let discussed the implementation of Dynamic Source Routing (DSR) protocol using the Click modular router on a real life testbed consisting of laptops and wireless Ethernet cards. Finally described the modifications we have made to the DSR router to make it energy aware [3].

Large-scale peer-to-peer systems face security threats from faulty or hostile remote elements of computing. To fight back these threats, many such methods employ redundancy. If a single faulty entity can present several identities, it can switch a considerable system fraction, thereby undermining this redundancy. There is an approach to preventing these “Sybil attacks” is to have a trusted agency certify identities. This attack shows that, without a logically regionalspecialist, Sybil attacks are always likelybut under extreme and unrealistic assumptions of resource parity and coordination among entities [4].

A mobile ad hoc network is a mobilegroup, wireless nodes which obligingly form a network independent of any fixed infrastructure or centralized management. In specific, a Manet has no base stations, a node lead intoin a straight line with nodes within wireless range and indirectly with all other nodes using a dynamically-computed, multi-hop route via the Manet of other nodes. Simulation and experimental results are combined to show that energy and Bandwidth is substantively different metrics and that resource utilization in Manet routing protocols is not fully addressed by bandwidth-centric study. This resultpresents a typical for assessing the energy consumption behaviourof mobile ad hoc networks. This model was used to test the energy consumption of two well-known Manet protocol of routing. Energy-aware enactment analysis is shown to provide new insights into costly protocol behaviours and suggests opportunities for improvement at the protocol and link layers [5].

In an advanced signature system the investigation about the security issues related to the Optimized Link State Routing Protocol one example of a proactive routing protocol for MANETs has been done. Inventory the possible attacks against the integrity of the OLSR network routing structure, and recent technique for make safe the network. In particular, high and mighty that a mechanism for routing message authentication (digital signatures) has been deployed, and concentrated on the problem where otherwise “trusted" nodes have been compromised by attackers, which could then inject false (however correctly signed) routing messages. The main approach is based on authentication checks of information injected keen on the network, and reprocess of this data by a node to prove its link state at a far alongthe time. As a final point, the directly above and the remaining susceptibilities of the proposed solution are synthetized. [6].

Ad hoc wireless networks enable new and exciting uses, but also importantpositionof technical challenges. In this thing gave a brief summary of ad hoc wireless networks and their applications with a particular emphasis on constraints of energy. Then the discussion about the recent things in the link, severalaccesses, network, and the application protocols for these networks. Cross-layer design of these protocols is imperative to meeting emerging application requirements has been shown, particularly when energy is a limited resource [7].

The considerations of routing security in wireless sensor networks are attacks and countermeasures. Many sensor network routing protocols has proposed, but no one of them have been intended with security as a goal. Proposed the security goals for routing in wireless sensor networks, show how the attacks in contradiction of ad-hoc networks and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce and acquaint with two classes of novel attacks in contrast to sensor networks sinkholes and HELLO floods, and analyse the safety of the whole major sensor network routing protocols and also described the crippling attacks against all of them and suggest countermeasures and design considerations. This is the basic thing that such analysis of protected routing in sensor networks [8].

Greedy Perimeter Stateless Routing (GPSR), a novel routing protocol for wireless datagram networks that uses the positions of routers and a packet's destination to make packet advancingresults. GPSR makes avaricious forwarding results using only information about a router's immediate neighbours in the topology of the networks. When a packet touches a Under mobility's frequenttopologydeviations, GPSRcan use Local topology information to find correct new routes quickly. GPSR protocol and use wide spread simulation of mobile Wireless networks to match its enactment with that of DynamicSourceRoutinghasdescribed.Simulations Proved GPSR'sscalabilityon compactly deployed Wireless networks [9].

The Dynamic Source Routing protocol (DSR) is a simple and efficient routing protocol designed specifically for use in multi-hop wireless ad hoc networks of nodes of the mobile. DSR permits the network to be fully self-organizing and self-arranging, without the need for any in effect of network infrastructure or supervision. The protocol is self-possessed of the two contrivances of Route Discovery and Route Maintenance, which effortcomposed to allow nodes to find out and maintain source routes to arbitrary destinations in the ad hoc networks. The usage of basis routing permits packet routing to be trivially loop-free, evades the necessity for up-to-date routing data in the intermediate nodes through which packets are hold back, and permits nodes forwarding or listen in packets to cache the routing information in them for their own future use. Evaluated the operation of DSR through detailed simulation on a variety of movement and communication forms, and through putting into practice and significant experimentation in a physical outdoor ad hoc networking test bed have constructed in Pittsburgh, and have established the excellent enactment of the protocol. Design of DSR and provide a summary of some of our simulation and test bed implementation results for the protocol has been described [10].

Effective mitigation of denial of service (DoS) attack is a pressing problem on the online internet source. In many cases in point, DoS attacks can be prevented if the spoofed source IP address is traced back to its origin which allows assigning penalties to the offending party or isolating the compromised hosts and domains from the rest of the network. In this paper, shown that probabilistic packet marking of interest due to its efficiency and implement ability vis-a-vis deterministic packet marking and logging or messaging based schemes suffers under spoofing of the marking field in the IP header by the attacker which can impede traceback by the victim and also shown that there is a trade-off between the ability of the victim to localize the attacker and the severity of the DoS outbreak, which is symbolized as a function of the marking probability, path length, and traffic volume[11].

region where avaricious forwarding is difficult, the algorithm get better by routing around the perimeter of the region. By keeping state only about the local of the topology, GPSR scales improved in per-router state than shortest-path and ad-hoc routing protocols as the number of network destinations Increases.

III.EXISTING SYSTEM

A. SYSTEM OVERVIEW:

In the related work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but Vampires don't disrupt or change the discovered paths, instead using the previous valid network ways and protocol messages by complaining. Protocols that get the most out of power efficiency are also incorrect, since they depend oncooperative node behaviour and cannot optimize out malicious action.

[1] CAROUSEL ATTACK:

- Adversary put togetherthe packets with purposely make known to routing loops
- Sends packets in circles
- Goalsof the 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.

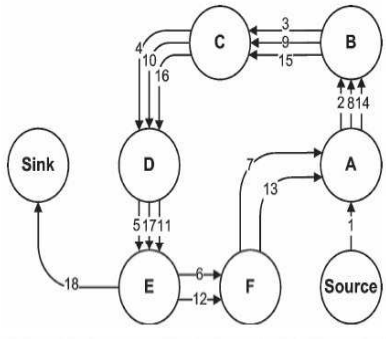

FIG 3.1.An honest route would exit the loop immediately from node E to the sink, but a hateful packet makes its way around the loop twice more before exiting.

- count along the shortest path between the adversary and packet destination.

Honest hop count = 3
Malicious hop count = 6

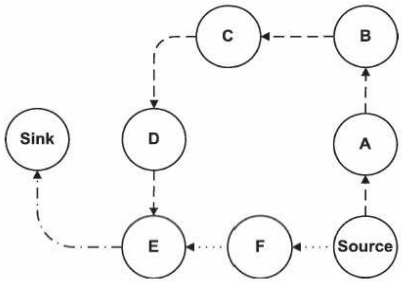

FIG 3.2. Honest route is dotted while malicious route is dashed. The last link to the sink is shared

DRAWBACKS:

- System can't achieve the good Quality of Service (QoS).
- Loss of Energy Management
- Loss of Time Management – Data Delivery will happen but can't predict the time.

B. ARCHITECTURE DIAGRAM:

It represents the architecture diagram of DETECTION OF VAMPIRE ATTACKS USING OPTIMAL ENERGY BOOST-UP IN WSNs.

[2] STRECH ATTACK:

- An enemyof the node constructs artificially stretched routes, potentially traversing every node in the network.
- Growthsof the packet path lengths, causing packets to be processed by a number of nodes that is independent of hop

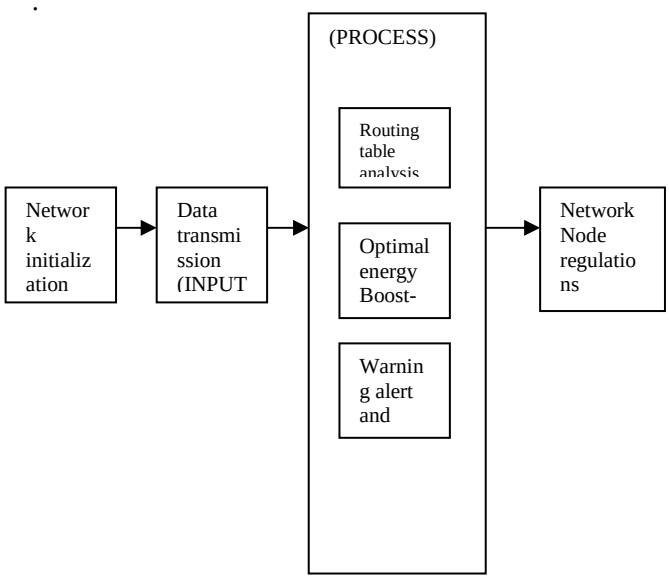

FIG 3.3.Architecture Diagram for the Detection of Vampire Attacks.

IV. PROPOSED SYSTEM

The simulation results quantifying the performance of several representative protocols in the presence of a single Vampire has been shown. Then, we modify an existing sensor network routing protocol to

provably bind the damage from Vampire attacks during packet forwarding.

Clean-Slate Sensor Network Routing:

• PLGP: a clean-slate secure sensor network routing protocol by Parno et al.

• The true fact version of the protocol is in danger to Vampire attacks.

• PLGP contains of a topology discovery phase, followed by a packet forwarding phase.

• Detection of deterministically organizes nodes into a tree that will later be used as an addressing scheme

a) repeated on a fixed schedule
b) Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme.
c) When discovery begins, each node has a limited view of the network the node knows by the only itself. Nodes find out their fellow citizen using nearest broadcast, and form ever expanding "neighborhoods," stopping when the entire network is a one group. Entire process, nodes build a tree of neighbor relationships and group membership that will later be used for addressing and routing.

ADVANTAGES OF PROPROSED SYSTEM:

- Energy management is enriched in the system.
- Quality of Service is achieved.
- Routing Table analysis is used to find the attacker.
- Time Complexity is reduced while compared with the existing system.

V. CONCLUSION AND FUTURE ENHANCEMENT

A new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes battery power. These attacks do not depend on particular protocols or putting into practice, but rather interpretation vulnerabilities in aamount of popular protocol programs. In the avoidance of data from Vampire attacks process it can only be able to detect and find the attacks has been done. The experimental results shows that the detection of the attacker using PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. It doesn't offer a fully satisfactory solution for Vampire attacks during the topology discovery phase. But by using the modification of PLGPa as Optimal Energy Boost-Up Protocol (OEBP), can further improve the prevention rate and finding the attacker, and can topology can be discovered and reconfigured accurately and the paper could be extended in future by including the following methods and algorithms,

- Proof submission algorithm (receives acknowledgement and combines as the proof)
- Topology discovery based on the attacks
- Topology reconfiguration

Vampire attack detection algorithm:

- Optimal energy Boost-up protocol (OEBP). This predicts the vampire attacks based on the existing behavior and finds optimal path and optimal topology discovery.
- Schedules the energy consumption and need of energy if any node performs vampire.
- Topology verification.

REFERENCES

1) Eugene Y. Vasserman and Nicholas Hopper, "Vampire attacks: Draining Life from Wireless Ad Hoc Sensor Network," IEEE Transactions On Mobile Computing, Vol. 12, No. 2, Feb 2013
2) 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.
3) S. Doshi, S. Bhandare, and T.X. Brown, "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) J.R. Douceur, "The Sybil Attack," Proc. Int'l Workshop Peer-to-Peer Systems, 2002.

5) 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.

6) D. Raffo, C. Adjih, T. Clausen, and P. Mu¨ hlethaler, "An Advanced Signature System for OLSR," Proc. Second ACM Workshop Security of Ad Hoc and Sensor Networks (SASN), 2004.

7) A.J. Goldsmith and S.B. Wicker, "Design Challenges for Energy-Constrained Ad Hoc Wireless Networks," IEEE Wireless Comm. vol. 9, no. 4, pp. 8-27, Aug. 2002.

8) C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l Workshop Sensor Network Protocols and Applications, 2003.

9) B. Karp and H.T. Kung, "GPSR: Greedy Perimeter Stateless Routing for Wireless Networks," Proc. ACM MobiCom, 2000.

10) D.B. Johnson, D.A. Maltz, and J. Broch, "DSR: The Dynamic Source Routing Protocol for Multihop Wireless Ad Hoc Networks," Ad Hoc Networking, Addison-Wesley, 2001.

11) Park and H. Lee, "On the Effectiveness of Probabilistic Packet Marking for IP Traceback under Denial of Service Attack," Proc. IEEE INFOCOM, 2001.

Thanmanam.P had completed B.Tech degree in Information Technology from Mahendra college of Engineering, Salem. Affiliated to Anna University. Pursuing his M.Tech degree in Information Technology. His area of Interest is on Network Security.

M. Suguna is an associate professor in SNS College of Technology, Coimbatore. She had completed a BE in Computer Science Engineering from Kumaraguru College of Technology, Coimbatore and ME degree in Computer Science Engineering from Government College of Technology, Coimbatore. Her area of interest are Image Processing and Soft Computing.