ISSN (Online) : 2319 - 8753
ISSN (Print) : 2347 - 6710

IJIRSET

International Journal of Innovative Research in Science, Engineering and Technology

Volume 3, Special Issue 3, March 2014

2014 International Conference on Innovations in Engineering and Technology (ICIET'14)

On 21st & 22nd March Organized by

K.L.N. College of Engineering, Madurai, Tamil Nadu, India

# Maximizing Lifetime of Nodes in Wireless Ad Hoc Sensor Network by Preventing Vampire Attack

A.Vincy, V.Uma Devi

PG Student, Department of Computer Science, Arunai Engineering College, Tiruvannamalai, Tamilnadu, India

Assistant Professor,, Department of Computer Science, Arunai Engineering College, Tiruvannamalai, 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. This explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes' battery power.The Vampire attacks are not exact to any specific protocol.The Vampire attacks, which are not easy to detect. The proposed approach consists of two phases. In the first, phase detecting and preventing denial of service attack based on secret sharing(SS) algorithm. In the second phase, increasing network lifetime based on switching the node states. The data verification process is provided at both the server and client side. It provides comparatively high security. It reduced the intruder spoofing.

**KEYWORDS***:* Attack,routing protocols,system security.

## I. INTRODUCTION

Wireless Sensor networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios.

A new emerged technology using sensing and enveloping computing is Ad hoc wireless networks. An ad hoc network typically refers to any set of networks where all devices have equal status on a network. The concept is Mobile communicates directly with access points.

The advantage of ad hoc networks are Ease of deployment Speed of deployment Decreased dependence on infrastructure.

A collection of two or more devices equipped with wireless communications and networking capability supports anytime and anywhere computing. The main work of proposed system is based on the routing or medium access control levels according to the rejection of communication in a network. There are various kind of attack based on that only routing protocol is developed. The intruder in the network can able to disable the whole networks by quickly draining nodes' battery power.

Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance vector, source routing, and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution.

## II. RELATED WORK

The proposed attack prevents nodes from entering a low-power sleep cycle, and thus depletes their batteries faster. Newer research on"denial-of-sleep" only considers attacks at the MAC layer. Additional work mentions resource exhaustion at theMAC and transport layers but only offers ratelimiting and elimination of insider adversaries as potentialsolutions. There is a literature on attacks anddefenses against quality of service (QoS) degradation, attacks that produce long-term degradation in networkperformance. Thefocus of this work is on the transport layer rather than routing protocols, so these defenses are not applicable.Vampires do not drop packets, the qualityof the malicious path itself may remain high. On denial of service in ad hoc wireless networks has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration. A seminal work on lifetime maximization in wireless sensor networks is, where routing of sensor data flows with givensampling rates is addressed, albeit with no consideration of estimation constraints.

### A. Attacks on Various Type of Protocols

Assume thereare numbers of people communicating in the world, they use various languages, various machines they use, the number of ways in which they transmit data and the different software they use. We would never be able to communicate worldwide if there were no ‘standards’ governing the way we communicate and the way our machines treat data. These standards are sets of rules. There are rules governing how data is transferred over networks, how they are compressed, how they are presented on the screen and so on. These set of rules are called protocols. There are many protocols, each one governing the way a certain technology works. For example, the IP protocol gives a set of rules governing the way computers use IP packets to send data over the Internet.

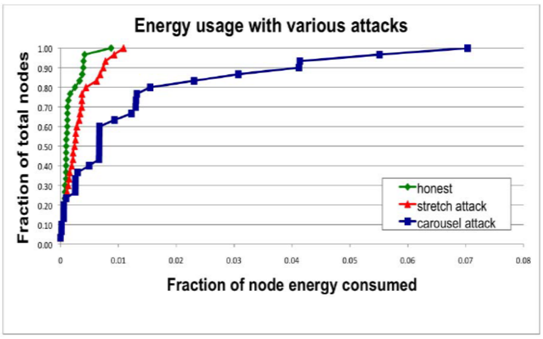


Fig 1Node energy distribution under various attack scenarios

### B. Carousel Attack

In this attack, an adversary sends a packet with a route composed as a series of loops, such that the samenode appears in the route many times. This strategy can be used to increase the route length beyond the number ofnodes in the network, only limited by the number of allowed entries in the source route. An example of thistype of route. In fig 2 malicious nodes 0 carries out a carousel attack, sending a single message to node 19 (which does not have to be malicious). Note the drastic increase in energy usage along the original path.

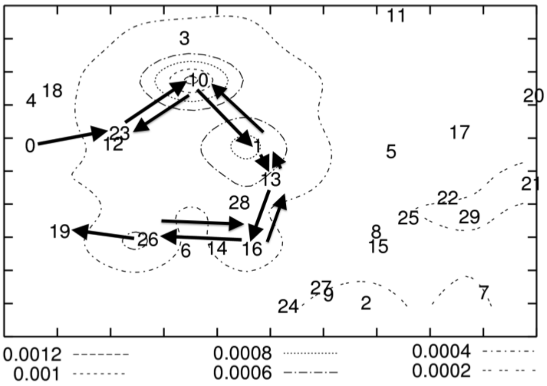


Fig 2Carousel attack

### C. Stretch Attack

Another attack in the same vein is the stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes.

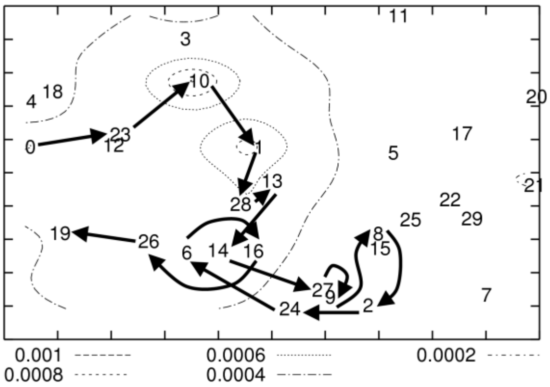


Fig 3 stretch attack

### DISTANCE-VECTOR ROUTING PROTOCOL

A distance-vector routing protocol needs that a router informs its neighbors of topology changes periodically. Compared to link-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead.The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network.Routing is the process by which a packet gets from one location to another. To route a packet, a router needs to know the destination address and on what interface to send the traffic out .When a packet comes into an interface on a router, it looks up the destination IP address in the packet header and compares it with its routing table. The routing table, which is stored in RAM, tells the router which outgoing interface the packet should go out to reach the destination network. Instead they use two methods:

1. Direction in which router or exit interface a packet should be forwarded.
2. Distance from its destination

Distance-vector protocols are based on calculating the direction and distance to any link in a network. "Direction" usually means the next hop address and the exit interface. "Distance" is a measure of the cost to reach a certain node. The least cost route between any two nodes is the route with minimum distance. Each node maintains a vector (table) of minimum distance to every node. The cost of reaching a destination is calculated using various route metrics. RIP uses the hop count of the destination whereas IGRP takes into account other information such as node delay and available bandwidth.

### D. *Advantage and Disadvantage*

Distance Vector is a clear  approach and easy to use, implement and maintain and does not require High-level knowledge to deploy. Moreover, it does not demand high bandwidth level to send their periodic updates as the size of the packets are relatively small. Furthermore, distance vector protocols do not require a large amount of CPU resources or memory to store the routing data.
The main drawbacks of Distance Vector are limited scalability due to slow convergence time, bandwidth consumption and routing loops.

### E. LINK-STATE ROUTING PROTOCOL

A link-state routing protocol is one of the two main classes of routing protocols used in packet switching networks for computer communications (the other is the distance-vector routing protocol). Examples of link-state routing protocols include open shortest path first (OSPF) and intermediate system to intermediate system (IS-IS).The link-state protocol is performed by every switching node in the network (i.e. nodes that are prepared to forward packets; in the Internet, these are called routers).
The basic concept of link-state routing is that every node constructs a map of the connectivity to the network, in the form of a graph, showing which nodes are connected to which other nodes. Each node then independently calculates the next best logical path from it to every possible destination in the network. The collection of best paths will then form the node's routing table.
This contrasts with distance-vector routing protocols, which work by having each node share its routing table with its neighbors. In a link-state protocol the only information passed between nodes is connectivity related.

### F. *Advantages*

Links-state routing protocols operate better in large, enterprise-level networks.
Link state convergence occurs faster than distance vector convergence.
They use multicasts (instead of broadcasts) to share routing information.
They support classless routing.

### G. *Disadvantage*

Link state protocols are more CPU- and memory-intensive. It have to maintain more tables in memory: a neighbor table, a link state database, and a routing table. When changes take place in the network, the routers must update the link state database, run the SPF algorithm, build the SPF tree, and then rebuild the routing table.

## III. SYSTEM DESIGN

### A.SYSTEM ARCHITECTURE

The architecture design describes the overall flow of the system. It explains all the main process such as denial of service attack, eliminating attack and secure file transfer.

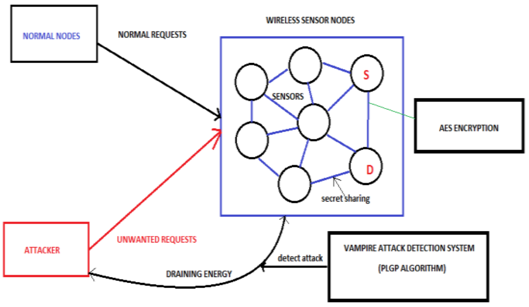


Fig 4 Architecture

### B. MODULE DESIGN

It includes the data verification, denial of service, intruder spoofing and secure file transfer.

1.Data-Verification:

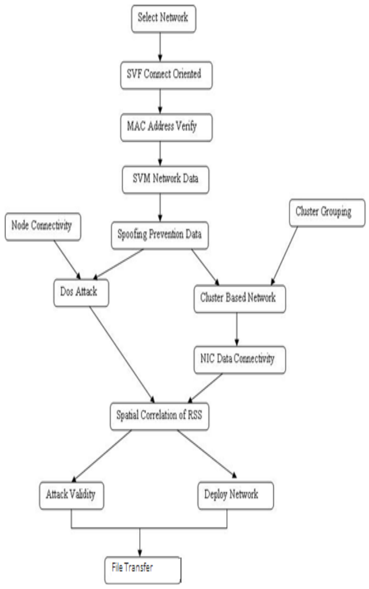
In data verification module, receiver verifies the path. Suppose data come with malicious node means placed in malicious packet. Otherwise data placed in honest packet. This way user verifies the data's.

The mechanism used is greedy mechanism where each node forwards a packet to the neighboring node that is closest to the destination. The Euclidean distance to the destination is generally used as metric.

2.Denial of service:

In computing, a denial-of-service attack or distributed denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.A denial-of-service attack is an attempt to make a machine or network resource unavailable to its intended users. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers.

This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. One common method of attack involves saturating the target machine with external communications requests, so much so that it cannot respond to legitimate traffic or responds so slowly as to be rendered essentially unavailable. Such attacks usually lead to a server overload. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.



**3.Trusting Topology Process:**

In this module we are forming a trusted topology. Choose a Node For that want to join trusted topology. Requested Node must be Submit a policy which is requiring a trusted node. Choose a Node for grant Permission for requested node which is already joined the trusted topology. Accept Node must be check the require policy which is submitted by Requested node. From this process we can filter the outsider attack into our topology. Now our topology keeps safe from the outsider attack.

GEOGRAPHIC ROUTING

Geographical routing uses location information to formulate an efficient route search toward the destination. Geographical routing is very suitable to sensor networks, where data aggregation is a useful technique to minimize the number of transmissions toward the base station by eliminating redundancy among packets from the different sources. It is much attractive for large multi-hop wirelessnetworks in which the nodes are not reliable and their network topology is frequently changing.

Geographical routing only requires the propagation of single hop topology information, like the best neighbor, to make correct forwarding decisions. Its localized approach reduces the need of maintaining routing tables, and hence reduces the control overhead.

It does not require flooding. Only nodes that lie within the designated forwarding zone are allowed to forward the data packet. The forwarding region can be defined by the source node or by the intermediate nodes to exclude nodes that may cause a detour while forwarding the data packet. The second property of geographical routing is its position based routing. Here a node requires knowing only the location information of its direct neighbor.

Location-based routing protocols are based on two principal assumptions:

• It is assumed that every node knows its own network neighbors positions.

• The source of a message is assumed to be informed about the position of the destination.

This technique for localized broadcasting of queries in geo-aware sensor networks makes use of the existing query routing tree and does not involve the creation of any additional communication channels. These algorithms require nodes toperiodically transmit HELLO messages to allow neighbors to know their positions. The location-based routing technique is very interesting because it operates without any routing tables. Furthermore, once the position of the destination is known, alloperations are strictly local, that is, every node is required to keep track only of its direct neighbor

**4.State of Each Node:**

Meta protocol have many states that is Begin state, Sleep state, Awake state, Rest state, Working state and halt state. Begin state is initial state for all the nodes which is joined into topology. All the nodes should be shift from begin state to sleep state. The node which is stay into sleep state that can shift to awake state. The Awake state nodes may shift to either working state or back to sleep state. Working state nodes only can transfer the files between them. Working state nodes may be shift to either rest state or back to awake state. The rest state nodes can move to either sleep state or return to working state.

**5.Intrude Process:**

In this module we are eliminate a intruder for keep trusted topology structure. After joined into topology the node may become a intruder. Which node change their kernel level information that node will be consider as intruder. Which node makes DOS Attack that will consider as intruder. The intruder will be sent out from our topology. From this process we can filter the insider attack into our topology. Now our topology keeps safe from the insider attack.

**6.Secure File Transfer:**

Trusted topology network nodes can transform files between them because our topology network gives a full trustworthy. Working state node can only transfer files between them. Remaining node cannot transfer files between them. Which node wants to be communicating to other node those two nodes must come to working state. So that we can increase the network life time. Our topology include many states for each node from this process we can achieve the lifetime increase of each network.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 when 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.

## IV. DISCUSSIONRESULTS

A hierarchical structuring of relations may result in more classes and a more complicated structure to implement. Therefore it is advisable to transform the hierarchical relation structure to a simpler structure such as a classical flat one. It is rather straightforward to transform the developed hierarchical model into a bipartite, flat model, consisting of classes on the one hand and flat relations on the other. Flat relations are preferred at the design level for reasons of simplicity and implementation ease. There is no identity or functionality associated with a flat relation. A flat relation corresponds with the relation concept of entity-relationship modeling and many object oriented methods.

**Constraints in Analysis**

- Constraints as Informal Text
- Constraints as Operational Restrictions
- Constraints Integrated in Existing Model Concepts
- Constraints as a Separate Concept
- Constraints Implied by the Model Structure

**Existing Graph**

The network is composed of 30 nodes and a single randomly positioned Vampire. Results shown are based on a single packet sent by the attacker.

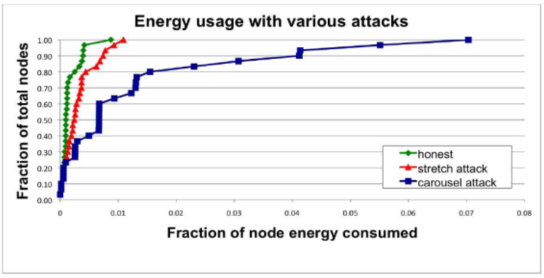


Fig 5 Node energy distribution under various attack scenarios

**Proposed Graph**

PLGP offers performance comparable to BVR in the average case.PLGPa includes path attestations, increasing the size of every packet, incurring penalties in terms of bandwidth use, and thus radio power. The bandwidth overhead of our attestation scheme is minimal, as chain signatures are compact.

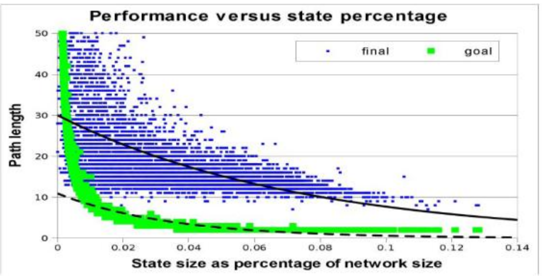


Fig 5.2 Loose source routing performance

## V. CONCLUSION AND FUTURE SCOPE

### A.CONCLUSION

In this we concentrate on the energy efficient protocols they divide the network to efficiently maintain the energy consumption of sensor nodes and perform data aggregation and fusion in order to decrease the number of transmitted messages to the sink. that have been developed for WSNs.They ensure optimized such as delay bound, energy efficiency, and low bandwidth consumption while achieving energy efficiency in WSNs applications. The position based routing protocol is an energy efficient mechanism where only the minimum processing is done by the sensor node.Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases from between 50 to 1,000 percent.

### B. *Scope for Future Work*

In the near future, we will evaluate the interactions of ASCENT with new MAC mechanisms, and the use of robust statistical techniques to improve on-line link quality estimation. We will also investigate the use of load balancing techniques to distribute the energy load, and explore the use of wider area links to detect network partitions. More generally, we are interested in understanding the relationships between topology control mechanisms, like ASCENT, and different routing strategies. This work is an initial foray into the design of self-configuring mechanisms for wireless sensor networks. Our distributed sensing network simulations and experiments represent a non-trivial exploration of the problem space. Such techniques will find increasing importance as the community seeks ways to exploit the redundancy offered by cheap, widely available micro sensors, as a way of addressing new dimensions of network performance such as network-lifetime .

This chapter conclude the project that it is high secured this chapter also described the idea about the future enhancement that to increase the lifetime of node with efficient and high security**.**

## REFERENCES

1.H. Chan and A. Perrig, *"Security and Privacy in SensorNetworks,"* Computer, vol. 36, no.10, pp. 103-105, Oct. 2003.

2.J.-H. Chang and L. Tassiulas, *"Maximum Lifetime Routing inWireless Sensor Networks,"* IEEE/ACM Trans. Networking, vol. 12,no. 4, pp. 609-619, Aug. 2004.

3.J. Deng, R. Han, and S. Mishra, *"Defending against Path-BasedDoS Attacks in Wireless Sensor Networks,"* Proc. ACM WorkshopSecurity of Ad Hoc and Sensor Networks, 2005.

4.C. Karlof and D. Wagner, *"Secure Routing in Wireless SensorNetworks: Attacks and Countermeasures*," Proc. IEEE Int'l WorkshopSensor Network Protocols and Applications, 2003.

5.A.D. Wood and J.A. Stankovic, *"Denial of Service in SensorNetworks,"* Computer, vol. 35, no. 10, pp. 54-62, Oct. 2002.

6.D.R. Raymond and S.F. Midkiff, *"Denial-of-Service in WirelessSensor Networks: Attacks and Defenses,"* IEEE Pervasive Computing,vol. 7, no. 1, pp. 74-81, Jan.-Mar. 2008.

7.Y.-C. Hu, D.B. Johnson, and A. Perrig, *"SEAD: Secure EfficientDistance Vector Routing for Mobile Wireless Ad Hoc Networks,"*Proc. IEEE Workshop Mobile Computing Systems and Applications,2002.

8. 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.