Defending against Energy Draining attack in Wireless Ad-Hoc Sensor Networks

[I]P.Suthahar, [II]R.Bharathi
[I]PG Student ME (CSE), M.Kumarasamy College of Engineering, (Autonomous) Karur, Tamil Nadu, India
[II]Assistant Professor, Dept. of CSE, M.Kumarasamy College of Engineering (Autonomous)

Abstract

Network survivability is the ability of a network keeping connected under failures and attacks, which is a fundamental issue to the design and performance evaluation of wireless ad hoc networks. Ad-hoc low power wireless networks are in research in both sensing and pervasive computing. The proposed method discusses about resource depletion attacks at the routing protocol layer, which drains battery power. The motivation of a large portion of research efforts has been to maximize the lifetime of the network, where network lifetime is typically measured from the instant of deployment to the point when one of the nodes has exp¬¬¬anded its limited power source and becomes in-operational – commonly referred as first node failure. A novel approach for routing protocols, affect from attack even those designed to be protected, be short of protection from these attacks, which call Vampire attacks, which permanently disable networks by quickly draining nodes battery power. These energy draining attacks are not specific to any specific protocol which are disturbing, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol compliant messages. There are a lot of protocols developed to protect from Denial of Service attack, but it is not completely possible. One such Denial of Service attack is Vampire attack-Draining of node life from wireless ad-hoc sensor networks. This paper presents a method to tolerate the attack by using the Cluster Head. In case of any energy draining attack, the Cluster Head engages in the situation and delivers the packet to destination without dropping the packet. Thus providing a victorious and reliable message delivery even in case of Vampire attack. A novel PLGP method is proposed to mitigate the battery power draining attacks by improving the existing routing protocol.

Keywords

Ad-hoc sensor network, carousal attack, denial of service, stretch attack, routing, vampire attack, PLGP, Security

I. Introduction

Wireless ad-hoc Sensor Networks provide one of the missing connections between the Internet and the physical world. One of the fundamental problems in sensor networks is the calculation of coverage. Exposure is directly related to coverage in that it is a measure of how well an object, moving on an arbitrary path, can be observed by the sensor network over a period of time. In addition to the informal definition, a formal definition is defined for exposure and study of WSN properties. An efficient and effective algorithm is developed for calculation in sensor networks, specifically for finding minimal exposure paths. The minimal exposure path provides valuable information about the worst case exposure-based coverage in sensor networks. The algorithm works for any given distribution of sensors, sensor and intensity models, and characteristics of the network. It provides an unbounded level of accuracy as a function of run time and storage.

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. Over View

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

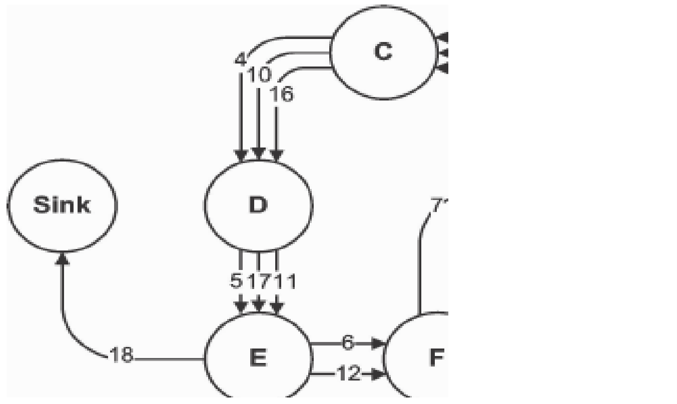

Fig. 1: An honest node would exit the loop immediately from node, but a malicious packet makes its way around the loop twice more before exiting.

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. Clearly, security mechanisms must give special effort to be communication efficient in order to be energy efficient. The proposed scale of sensor networks poses a significant challenge for security mechanisms. Simply networking tens to hundreds of thousands of nodes has proven to be a substantial task. Providing security over such a network is equally challenging. Security mechanisms must be scalable to very large networks while maintaining high computation and communication efficiency. Depending on the function of the particular sensor network, the sensor nodes may be left unattended for long periods of time.

In our first attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack, since it sends packets in circles as shown in Fig. 1. 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. In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We call this the stretch attack, since 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.

An example is illustrated in Fig.2. Results show that in a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overhead packets, we assume that only messages originated by adversaries may have maliciously composed routes.

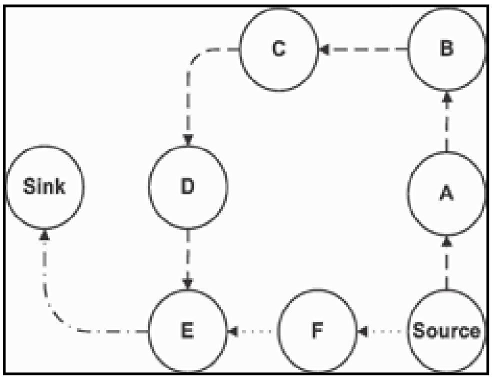

Fig. 2: Honest route is dotted while malicious route is dashed. The last link to the sink is shared.

III. Protocols and Attacks

In this section we discuss various protocols proposed for security of wireless sensor networks by different researchers. We do not imply that power draining itself is novel, but rather that these attacks have not been rigorously defined, evaluated, or mitigated at the routing layer. A very early mention of power exhaustion can be found in, as "sleep deprivation torture." As per the name, 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 the MAC and transport layers but only offers rate limiting and elimination of insider adversaries as potential solutions. Malicious cycles (routing loops) have been briefly mentioned, but no effective defenses are discussed other than increasing efficiency of the underlying MAC and routing protocols or switching away from source routing.

Even in non-power-constrained systems, depletion of resources such as memory, CPU time, and bandwidth may easily cause problems. A popular example is the SYN flood attack, wherein adversaries make multiple connection requests to a server, which will allocate resources for each connection request, eventually running out of resources, while the adversary, who allocates minimal resources, remains operational (since he does not intend to ever complete the connection handshake). Such attacks can be defeated or attenuated by putting greater burden on the connecting entity (e.g., SYN cookies, which offload the initial connection state onto the client, or cryptographic puzzles. These solutions place minimal load on legitimate clients who only initiate a small number of connections, but deter malicious entities who will attempt a large number. Note that this is actually a form of rate limiting, and not always desirable as it punishes nodes who produce burst traffic but may not send much total data over the lifetime of the network. Since Vampire attacks rely on amplification, such solutions may not be sufficiently effective to justify the excess load on legitimate nodes.

There is also significant past literature on attacks and defenses against quality of service (QoS) degradation, or RoQ attacks, that produce long-term degradation in net- work performance. The focus of this work is on the transport layer rather than routing protocols, so these defenses are not applicable. Moreover, since Vampires do not drop packets, the quality of the malicious path itself may remain high (although with increased latency). Other work 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, making our work tangential to the research mentioned above. Protocols that define security in terms of path discovery success, ensuring that only valid network paths are found, cannot protect against Vampire attacks, since Vampires do not use or return illegal routes or prevent communication in the short term. Current work in minimal-energy routing, which aims to increase the lifetime of power-constrained networks by using less energy to transmit and receive packets (e.g., by minimizing wireless transmission distance) is likewise orthogonal: these protocols focus on cooperative nodes and not malicious scenarios. Additional on power-conserving MAC, upper layer protocols, and cross-layer cooperation. However, Vampires will increase energy usage even in minimal-energy routing scenarios and when power- conserving MAC protocols are used; these attacks cannot be prevented at the MAC layer or through cross-layer feedback. Attackers will produce packets which traverse more hops than necessary, so even if nodes spend the minimum required energy to transmit packets, each packet is still more expensive to transmit in the presence of Vampires. Our work can be thought of attack-resistant minimal-energy routing, where the adversary's goal includes decreasing energy savings. The effect of denial or degradation of service on battery life and other finite node resources has not generally been a security consideration, making our work tangential to the research mentioned above.

Carousel Attack

In this attack, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. 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. An example of this type of route is in Fig.3 the thick path shows the honest path and thin shows the malicious path.

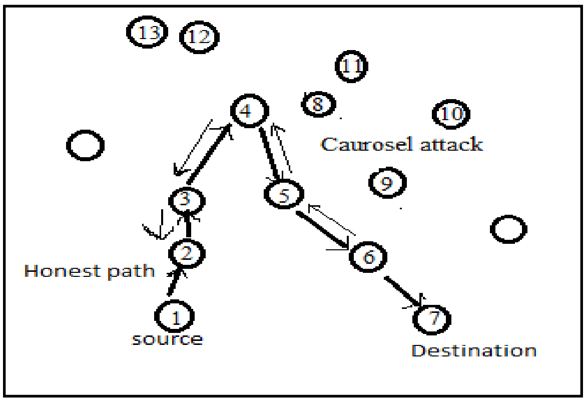

Fig. 3: shows the carousel attack same node appears in the route many times.

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. In the example given below honest path shown with thick lines and adversary or malicious path with thin lines. The honest path is very less distant but the malicious path is very long to make more energy consumption.

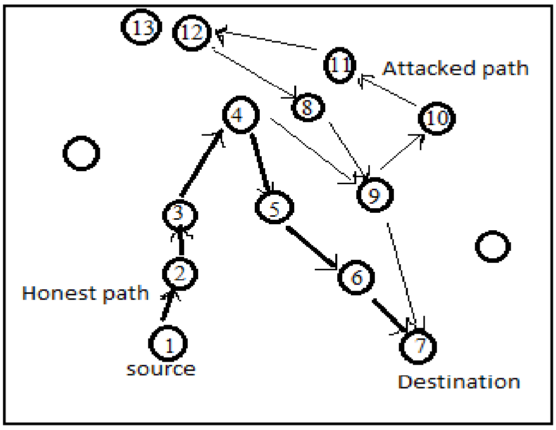

Fig. 4: Shows Stretch attack with two different paths from source to destination.(4-9-10-11-12-8-9—long route).

Per-node energy usage under both attacks is shown in Fig.5. As expected, the carousel attack causes excessive energy usage for a few nodes, since only nodes along a shorter path are affected. In contrast, the stretch attack shows more 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.

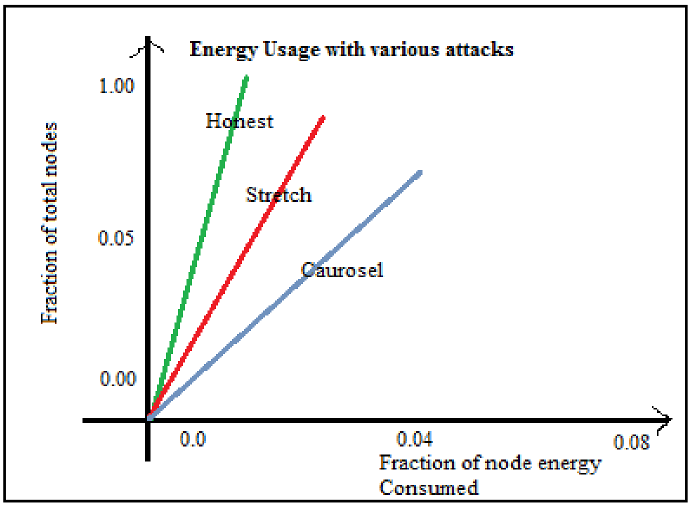

Fig. 5: Node Energy Distribution Under Various Attack Scenarios

IV. Stateful Protocols and their Attacks

A stateful protocol is where nodes are aware of their topology, its state, forwarding decisions. It requires the server to record the transaction so they can be recalled or resumed. Two important classes are link state and distance –vector. Example of link-state is OLSR and example of distance-vector is DSDV. Both these protocols are proactive, which routes to all reachable nodes in the network and minimizes the initial delay. OLSR keeps the record of up and down state of links and flood routing updates. DSDV is also known as Distributed Bellman-Ford or RIP (Routing Information Protocol). Every node maintains a routing table that contains all available destinations, the next node to reach to destination, the number of hops to reach the destination and periodically send table to all neighbors to maintain topology. Both these protocols are immune to carousel and stretch attacks. In fact, any time adversaries cannot specify the full path, the potential for Vampire attack is reduced. Two types of attacks in stateful protocol are directional antenna attack and malicious discovery attack. Directional antenna attack: In this the vampires have little control over the packets progress, but they still waste energy by restarting a packet in various parts of network. They will deposit the packets in arbitrary path of network due to this energy is consumed, O(d) where d is the network diameter, d/2 .It is also considered as half worm hole attack. Packet leashes cannot prevent this kind of attack since they are not meant to protect against malicious message source but only intermediary. Malicious Discovery Attack: It is also called as spurious rote discovery. Both AODV and DSR are vulnerable to this attack since nodes may initiate discovery at any time, not just during the topology change. This type of attack becomes serious when nodes claim that long distance route has changed. This attack is trivial in open networks. Packet leashes cannot prevent this type of attack. This is similar to route flapping in BGP.

V. Stateless Protocols and their Attacks

A stateless protocol does not require the server to retain session information or status about each communications partner for the duration of multiple requests. It is communication protocol that treats ach request as an independent transaction that is unrelated to any previous request so that the communication consists of independent pairs of requests and responses. The two most common types of attacks are Carousel attack shown in Figure [1] and Stretch attack shown in Figure [2]. It is called Stretch attack, since 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. The carousel on the other hand sends packets in circles. 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.

VI. Clean State Secure Routing Protocol (PLGP)

The PLGP protocol is modified as clean state secure routing protocol such that they can resist vampire attacks during the forwarding. PLGP was vulnerable to vampire attacks even though they were said to be secured. When the route discovery begins each node has a limited view about the network. As already said nodes discover the other nodes in a group by broadcasting a certificate id, signed by the public key of the online authority, thus forming a single group and a tree structure that will be used for addressing and routing. All nodes compute the same address as the other odes they also learn each other's virtual address as well as their cryptographic keys. The final address is verifiable after the network convergence and all forwarding decisions can be independently verified. PLGP consists of a topology discovery phase, followed by a packet forwarding phase, with the former optionally repeated on a fixed schedule to ensure that topology information stays current. (There is no on- demand discovery.) Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. When discovery begins, each node has a limited view of the network—the node knows only itself. Nodes discover their neighbors using local broadcast, and form ever expanding "neighborhoods," stopping when the entire network is a single group. Throughout this process, nodes build a tree of neighbor relationships and group member- ship that will later be used for addressing and routing.

At the end of discovery, each node should compute the same address tree as other nodes. All leaf nodes in the tree are physical nodes in the network, and their virtual addresses correspond to their position in the tree (see Fig. 6). All nodes learn each others' virtual addresses and cryptographic keys. The final address tree is verifiable after network convergence, and all forwarding decisions can be independently verified. Furthermore, assuming each legitimate network node has a unique certificate of membership (assigned before network deployment), nodes who attempt to join multiple groups, produce clones of themselves in multiple locations, or otherwise cheat during discovery can be identified and evicted.

A. Provable Security Against Vampire Attacks

Here, we modify the forwarding phase of PLGP to provably avoid the above-mentioned attacks. First we introduce the no-backtracking property, satisfied for a given packet if and only if it consistently makes progress toward its destination in the logical network address space. More formally:

Definition 1. No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network. (Maliciously induced route stretch is bounded to a factor of 1.)

This does not imply that every packet in the network must travel the same number of hops regardless of source or destination, but rather that a packet sent to node D by a malicious node at location L will traverse the same number of hops as a packet sent to D by a node at location L that is honest. If we think of this in terms of protocol execution traces, no-backtracking implies that for each packet in the trace, the number of intermediate honest nodes traversed by the packet between source and destination is independent of the actions of malicious nodes. Equivalently, traces that include malicious nodes should show the same network- wide energy utilization by honest nodes as traces of a network with no malicious actors. The only notable exceptions are when adversaries drop or mangle packets en route, but since we are only concerned with packets initiated by adversaries, we can safely ignore this situation: "premangled" packets achieve the same result—they will be dropped by an honest intermediary or destination.

No-backtracking implies Vampire resistance. It is not immediately obvious why no-backtracking prevents Vampire attacks in the forwarding phase. Recall the reason for the success of the stretch attack: intermediate nodes in a source route cannot check whether the source-defined route is optimal, or even that it makes progress toward the destination. When nodes make independent routing decisions such as in link-state, distance-vector, coordinate-based, or beacon-based protocols, packets cannot contain maliciously composed routes. This already means the adversary cannot perform carousel or stretch attacks— no node may unilaterally specify a suboptimal path through the network. However, a sufficiently clever adversary may still influence packet progress. We can prevent this interference by independently checking on packet progress: if nodes keep track of route "cost" or metric and, when forwarding a packet, communicate the local cost to the next hop, that next hop can verify that the remaining route cost is lower than before, and therefore the packet is making progress toward its destination. (Otherwise we suspect malicious intervention and drop the packet.) If we can guarantee that a packet is closer to its destination with every hop, we can bound the potential damage from an attacker as a function of network size. (A more desirable property is to guarantee good progress, such as logarithmic path length, but both allow us to obtain an upper bound on attack success.)

Definition 2. The hop count of packet p received or forwarded by an honest node, is no greater than the number of entries in p's route attestation field, plus 1.

When any node receives a message, it checks that every node in the path attestation 1) has a corresponding entry in the signature chain, and 2) is logically closer to the destination than the previous hop in the chain (see Function secure_forward_packet). This way, forward- ing nodes can enforce the forward progress of a message, preserving no-backtracking. If no attestation is present, the node checks to see if the originator of the message is a physical neighbor. Since messages are signed with the originator's key, malicious nodes cannot falsely claim to be the origin of a message, and therefore do not benefit by removing attestations.

VII. Modules

A. Topology Discovery and Cluster Head Selection

The topology we are going to use here is a mesh topology. In this case each node sends a message to the other nodes which it detects. Once a node detects the message it maintains a record to store information about the neighbor. Using multicast socket all nodes are used to detect their neighbor node. Cluster Head is elected based on range, mobility and battery power.

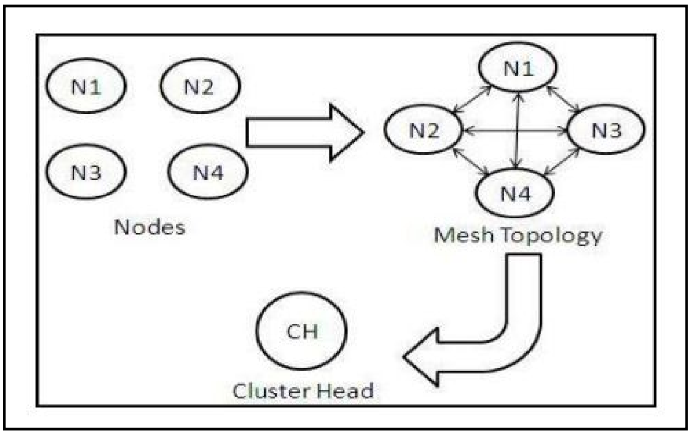

Fig: 6. Topology Discovery and Cluster Head Selection

B. Tree Formation and Route Discovery

Trees are formed as nodes form group. Each node starts with group size 1 and virtual address 0 so that one group is formed. Similarly other groups are also formed. When two nodes form a group their group size becomes 2 with one node taking a virtual address 0 and other taking the address 1.Each group can have their own group address. Example: node 0 in one group0 becomes 0.0 and node 0 in group 1 becomes 1.0. Each time a group is added or merged the address of each node is lengthened by one bit . Thus a tree structure is formed with address in the network and node address as leaves. Generally small groups form with 1 node later they merge to form large groups.

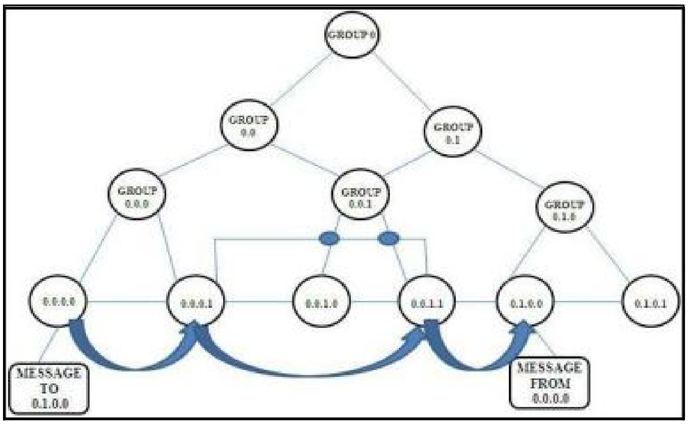

Fig: 7.Group identification.

For example when two groups merge to form a large group they broadcast their group id to each other and precede with the merge protocols. Each node stores the id of one or more nodes such that they can know that the other group exists such that every node within a group will end up with the next-hop path to every other group as in distance vector. Thus a tree is formed and the route is chosen in this manner until all network nodes are members of single group. By the end of this phase each node will

C. Forwarding the Packets

During this phase each node is independent of other node and hence the decision made by them is also independent. When a node receives a packet it determines the next hop by finding the most significant bit(MSB) address as it differs from the message originators address as it differs from the originators address.

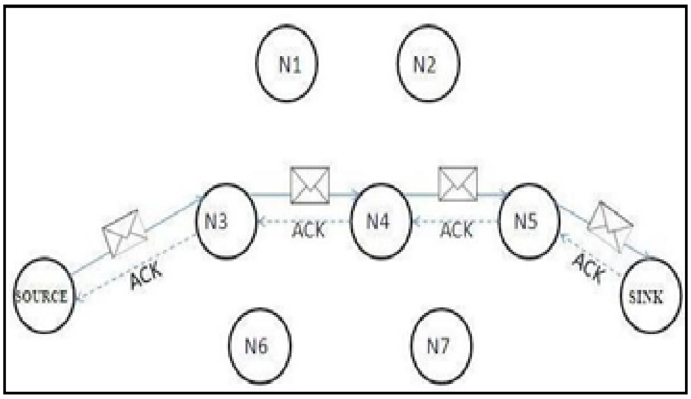

Fig: 8.Message traversal in normal situation.

When a packet is moving within a group and when they want to move to the next group they shortens the logical distance to destination since their address must be close to the destination.

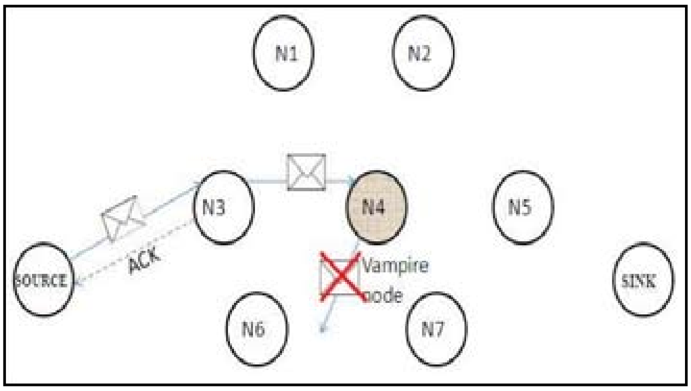

Fig: 9. Vampire Attack leading to message drop.

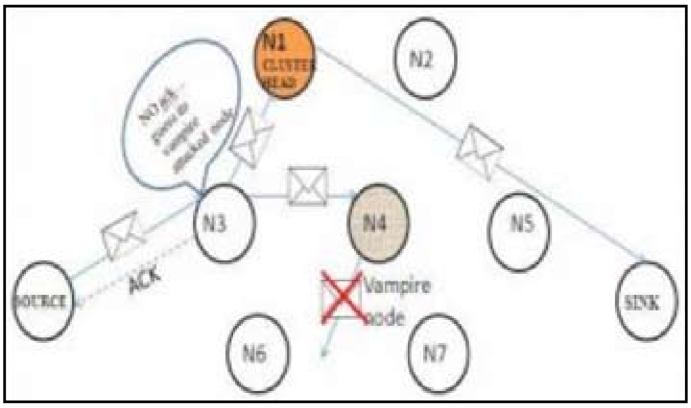

Fig: 10. After N trials node N3 sends data to cluster head (chosen based on highest coverage range, battery power) which sends data to sink.

VIII. Conclusion

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 PLGP the first sensor network routing protocol that provably bounds damage from vampire attacks by verifying the packets towards the destination. We have not offered a fully satisfactory solution for Energy draining attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGP. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

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] *"The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns, 2012*

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

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

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

[6] *T. Aura, "Dos-Resistant Authentication with Client Puzzles," Proc.Int'l Workshop Security Protocols, 2001.*

[7] *J. Bellardo and S. Savage, "802.11 Denial-of-Service Attacks: Real Vulnerabilities and Practical Solutions," Proc. 12th Conf. USENIX Security, 2003.*

[8] *I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ. , 1999.*

[9] *J.W. Bos, D.A. Osvik, and D. Stefan, "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.*

[10] *H.Chan and A. Perrig, "Security and Privacy in Sensor Networks," Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.*

[11] *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.*

[12] *T.H. Clausen and P. Jacquet, Optimized Link State Routing Protocol (OLSR), IETF RFC 3626, 2003.*

[13] *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.*

[14] *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.*

Author's Profile

Suthahar Ponnuchamy is a PG Student of Computer Science and Engineering department at M.Kumarasamy College of Engineering, Karur, Tamil Nadu. He received his B.Tech Degree in Information Technology in 2007at Anna University, Chennai, Tamil Nadu. He is interested in distributed network security, privacy and anonymity and web services.