ISSN 2321-6905
JULY - 2015

International Journal of Science Engineering and Advance Technology

Challenging Leech Assault Commencing Wireless Adhoc Set of Connections

Kantheti Bhanu Prakash[1], Kumararaja Jetti [2]
[1] M.Tech (CSE), Bapatla Engineering College, A.P., India
[2]Assistant Professor, Department of Computer Science & Engineering, Bapatla Engineering College, A.P., India

Abstract
An ad hoc network could be a cluster of wireless nodes, during which every node will communicate over multi hop methods to the other node while not the assistance of any pre-existing infrastructure like base station or access points.Due to these feature unintended low power wireless networks area unit capable of device and pervasive computing that forms the wireless unintended sensor network. Unintended need no centralized administration that the network infrastructure will be shaped quickly and cheap started is required.Unintended networks area unit being employed in operation, emergency disaster relief and community networking. a crucial security issue that has been known in these networks is resource depletion attack at routing layer protocol. These attacks drain nodes battery power fully, in order that the network is for good disabled. Thus these attacks area unit termed as lamia attacks. at the same time as there exist several secure routing protocols, they're unable to shield the network from lamia attacks. Therefore as a shot to eliminate lamia attacks, 3 primary contributions has been introduced. i. analysis of the vulnerabilities of existing protocols. ii. Division of performance of assorted protocols within the existence of solitary lamia. iii. Modification of existing protocol to eat lamia attacks. Ad-hoc low- power wireless networks area unit. Associate degree exciting analysis direction in sensing and pervasive computing. Previous security adds this space has targeted totally on denial of communication at the routing or medium access management levels. This paper explores resource depletion attacks at the routing protocol layer, that for good disable networks by quickly exhausting nodes' battery power. These "Vampire" attacks aren't specific to any specific protocol, however rather deem the properties of the many fashionable categories of routing protocols. we discover that every one examined protocols area unit at risk of lamia attacks, that area unit devastating, troublesome to discover, and area unit straightforward to hold out mistreatment as few collectively malicious corporate executive causation solely protocol compliant messages. within the worst case, one lamia will increase network-wide energy usage by an element of O(N),Wherever N within the range of network nodes. We have a tendency to discuss ways to mitigate these sorts of attacks, together with a brand new proof-of-concept protocol that incontrovertibly bounds the injury caused by Vampires throughout the packet forwarding part.

Keywords—Ad hoc sensor network, routing, security, denial of service, vampire attack, PLGP

I. Introduction:

Ad-hoc wireless device networks (WSNs) promise raising new applications within the forthcoming future, like continuous property, present on-demand conniving power, and immediately-deployable communication for military and initial responders. Such networks already monitor environmental conditions, plant performance, and troop readying, to call many applications. Owing to their ad-hoc organization, wireless adhoc networks area unit specifically prone to denial of service (DoS) attacks,and an excellent deal of analysis has been done to reinforce survivability. Whereas these schemes will stop attacks on the network in short accessibility, they are doing not tackle attacks that have impact on long-run accessibility the foremost stable denial of service attack is to thoroughly eat nodes' batteries. this can be an occasion of a resource depletion attack, with battery power because the resource of attention. During this paper we have a tendency to take into account however routing protocols, still those designed to be secure, its lack protection from these attacks, that we have a tendency to decision as lamia attacks, as a result of the drain the life from networks nodes. These attacks area unit completely different from previously-studied Reduction of Quality(RoQ), Denial of Service(DoS), and routing infrastructure attacks as they are doing not disturb direct accessibility, however somewhat beat up time to thoroughly disconnect a network. whereas a number of the individual attacks area unit straightforward, and resource exhaustion and power-draining attacks are mentioned before , previous work has been principally restricted to different levels of the protocol stack, e.g. medium access management (MAC) or application layers, and to our discussion there's very little discussion, and no complete analysis or mitigation, of routing- layer supply exhaustion attacks. lamia attacks aren't

ISSN 2321-6905
JULY - 2015

protocol-specific, in this they are doing not rely on style properties or implementation faults of specific routing protocols, however rather utilize common properties of protocol categories like link-state, supply routing, geographic, distance vector, and beacon routing. Neither do these attacks rely on flooding the network with Brobdingnagian amounts of knowledge, however somewhat attempt to transmit as very little information as attainable to realize the most important energy drain, preventing a rate limiting resolution. as a result of Vampires build use protocol-compliant messages, these attacks area unit terribly difficult to discover and stop. A. Contributions this paper makes 3 main contributions. First, we have a tendency to fully assess the vulnerabilities of existing protocols to routing layer battery exhaustion attacks. We have a tendency to monitor that security measures to forestall lamia attacks area unit orthogonal to those wont to defend routing infrastructure, then offered secure routing protocols like SAODV, Ariadne and SEAD don't defend against lamia attacks. Existing work on secure routing {attempts makes associate degree attempt tries} to create positive that adversaries cannot impact path discovery to come back an invalid network path, but Vampires don't disturb or modification discovered methods, as a substitute mistreatment protocol compliant messages and existing valid network methods. Protocols that benefit of power potency also are inappropriate, as a result of they supported cooperative node behavior and can't optimize out malicious action. Second, we have a tendency to demonstrate simulation results quantifying the performance of most representative protocols within the presence of one lamia (insider adversary). Third, we modify associate degree existing device network routing protocol to incontrovertibly certain the injury from lamia attacks throughout packet forwarding part. B. summary within the remainder of this paper, we have a tendency to gift a sequence of more and more damaging lamia attacks, calculate the vulnerability of some example protocols, and propose the way to improve resilience. In supply routing protocols, we have a tendency to illustrate however a malicious packet supply will ready to specify methods through the network that area unit so much longer than best, wasting energy at middle nodes UN agency additional forward the packet supported the enclosed supply route. In routing method wherever forwarding choices area unit created severally by every node (as critical specific by the source), we have a tendency to suggest however aerial and hollow attacks will be wont to distribute packets to many remote network positions, forcing packet process at nodes that will not typically receive that packet in the slightest degree, and therefore rising network-wide energy Expenditure. Finally, we have a tendency to illustrate however associate degree someone will target not solely packet forwarding however additionally route and topology discovery phases — if discovery messages area unit flooded, associate degree someone will, for the price of one packet, consume energy at every node within the network. In our initial attack, associate degree someone composes packets with advisedly introduced routing loops. we have a tendency to decision it the carousel attack, since it sends packets in a circle as shown in Figure 1(a). It targets supply routing protocols by exploiting the restricted authentication of message headers at forwarding nodes, permitting one packet to continually traverse a similar set of nodes.

II. Related Work

In wireless unintended and device Networks all nodes area unit connected to every different in an exceedingly wireless manner. In unintended networks the nodes type dynamic topology relying upon the amount of nodes obtainable and therefore the location during which the network has been deployed. The networks encounter an outsized range of resource depletion attacks like denial of service (DoS), exhausting battery life, packet drop and lots of a lot of. Denial of Service attack has become quite common in gift wireless networks. The complete network information measure gets occupied owing to continuous requests sent by unwelcome person or malicious nodes. This generates significant traffic within the network. Multiple requests sent at the same time produce significant traffic within the network. Authentication puzzles area unit employed in order to see the node's honesty before they're allowed to use the complete information measure [5]. Exhausting of battery life is another resource depletion attack that ends up in the failure of network. Completely different routing protocols area unit at risk of differing types of attacks. End air A, a incontrovertibly secure on-demand supply routing protocol is employed to avoid the routing attacks [4]. Greek deity (a fresh start routing protocol) was introduced to supply security to the transmitted information, however it consisted of many short comings. This was corrected by End air A however the protection problems still exist. the complete network will be paralyzed by one malicious node which may modification the complete routing path. hollow and natural depression attacks increase the network energy usage by an outsized margin when put next to different attacks. Packet leashes are introduced so as to limit this unwanted energy expenditure within the network [2]. Temporal leashes and Geographical leashes are designed so as to minimize the energy drain owing to the hollow attacks. Temporal leashes limit the life of the

ISSN 2321-6905
JULY - 2015

packet whereas geographical leashes limit the space or vary the packet will cowl. Time synchronization could be a key feature during this methodology. Lack of correct time synchronization renders the strategy ineffective. Unintended Networks could also be mobile in nature. Since all the applications presently used area unit wireless in nature, unintended networks area unit principally deployed in an exceedingly cluster hierarchy with mobile nodes. The cluster heads may be selected based upon the energy present in them. Nodes that act as the cluster heads will require more energy than the member nodes. The energy of every node is measured while selecting a cluster head. The nodes with the optimum energy may also compete for acting as the cluster head [6]. The cluster head may be changed periodically depending upon the energy consumed. Routing protocols such as LEACH [7], Cluster-Based Energy-Efficient Routing Protocol without Location Information [8], etc., consider cluster heads to be the major part of communication and assign the clusters accordingly. Stretch and carousel attacks have become very common in every routing protocol. The energy depletion that takes place due to these two attacks is quite high. PLGP [1], a clean slate secure sensor network routing protocol has been designed to reduce the energy drain due to these stretch and carousal attacks. The protocol is designed mainly for the packet forwarding phase and not for the topology discovery. Since networks at present are mostly Wireless, the topology is dynamic in nature. The PLGP protocol makes sure that there is always packet progress, i.e., the packet always travels towards the destination without any back tracking. The route once travelled is not back tracked since each node verifies the packet header, for the previous node's details. Even though the nodes checked the packet header details, the malicious nodes or the intruders had the capacity to edit or delete certain details. These malicious nodes may also forward packets without adding their details. Attestations were added to overcome this problem. PLGPa added attestations to the packet, which are similar to signatures, every time the packet is forwarded. This way the nodes cannot modify the previous node's details and will have to add their own signature to forward it. Attestations added to the packet header made the header size larger thereby leading to difficulty in encryption, decryption and coding.

III. Energy Draining Attacks On Stateless And Stateful Protocol:

In the DSR[9] source node specifies the entire route in the packet header to a destination, so intermediate node's do not make independent forwarding decisions, instead of a route specified by the source. To forward a message, the intermediate node finds itself in the route and Transmits the message to the next hop. The fardel is on the source to ensure that the route is valid at the time of sending, and that every node in the route is a physical neighbor of the previous route hop. Both the carousel and stretch attacks are evaluated in a randomly generated 30- node topology. It causes delay as well as increase communication overhead and energy consumption in resource limited networks .The effect of denial or degradation of service on battery life and other finite node resources has not generally been a considered securely.Carousel attack: In this attack, a malicious node forward a packet with a route included a chain of loops, such that the packets traverse several times in the same route. This strategy can be used to increase the route length beyond the number of nodes in the network An example of this type of route is in Fig.3the thick path shows the honest path and thin shows the malicious path.

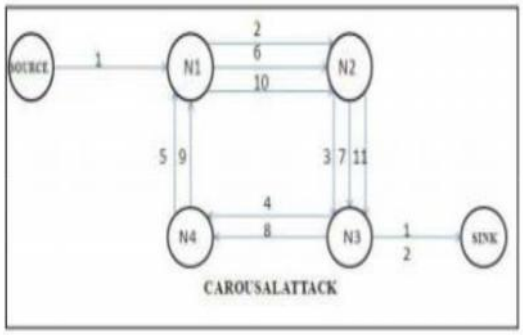


Figure. Carosuel attack

1) Stretch attack: Another attack in the same layer is the stretch attack, where a malicious node constructs falsely long source routes, causing packets to traverse a longer than optimal number of nodes. In this 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. 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.

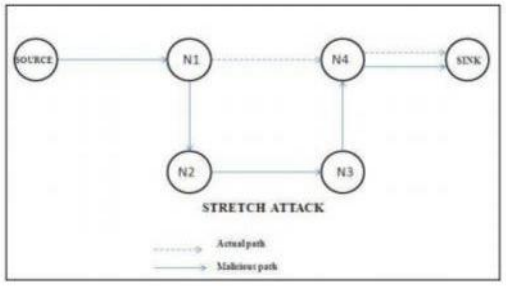


Figure. Stretch attack

IV. Proposed Work

The work proposed here is to prevent the packets from looping and stretch attacks. The energy that is

ISSN 2321-6905
JULY - 2015

Depleted due to these attacks plays a very important in the life time of the node. In the existing protocol, PLGP, the packet is checked for no backtracking by ensuring that every packet makes progress in the network. Each packet that is transmitted must travel towards the destination and must not re-trace the same path it has already traversed. The major drawback here is that certain malicious nodes can alter this path information thereby again leading to stretch and carousel attacks. To overcome these drawbacks PLGPa was introduced, which uses attestations that are added to the packet header. Attestations are similar to signatures. Every node has its unique signature. Therefore this is helps in adding extra security. In scenarios where the malicious node can duplicate the signature of another node, the PLGPa protocol is rendered useless.

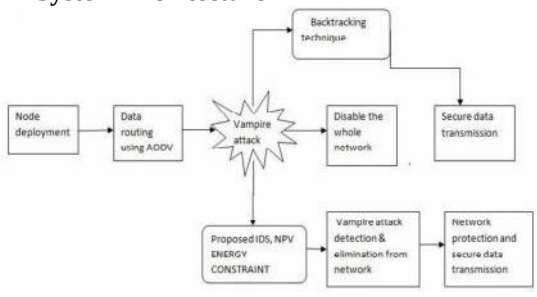
The main idea here is to generate a network which has very less energy depletion due to stretch and carousel attacks. A new protocol called MDSDV is proposed, which significantly reduces the energy depletion in the network due to such attacks. At first we generate a network with the required number of nodes. The nodes may be mobile or fixed in nature. The nodes are then connected using duplex links. The nodes are arranged in clusters in order to communicate efficiently. The cluster heads are elected at random. The cluster heads are changed based on LCC (Least Cluster Change). Here, the cluster head changes only when one of the following takes place; when two cluster heads are found within the same cluster or when the cluster head moves out of range of that particular cluster. The entire communication inside the cluster is only through the cluster head. Every cluster also has a cluster gateway. Two or more clusters are connected to each other only through this gateway. When a packet needs to be transmitted from one cluster to a different cluster, the gateway node obtains the packet from the cluster head and passes to its neighboring gateway. This is repeated until the destined cluster is reached. The Cluster head then transmits the packet to the destined member (sink) of that particular cluster.

Indexing number is added as a security to the packet header in order to avoid packet loops or stretch attacks. This is 8 bit in size therefore does not occupy much space in the header. This gets generated at random for every link therefore it cannot be duplicated. The indexing number is 0 in the beginning. Only when the link has been established the number is generated. The indexing number is changed after a particular time interval.

V. Methodology

In this paper, a layered approach is used to solve the problem with the vampire attacks. Vampire packet (malicious packet) monitoring is performed both in network layer (routing protocol layer) and Application layer. The network layer checking helps to point out the vampire packets from the network and the application layer checking helps to find out the vampires inside the running processes (ie, inside the node). Whenever an incoming packet is detected that is a vampire then the packet will not be forwarded and it will be discarded. Whenever a vampire is detected inside the node simply we can eliminate it. A clean-slate secure sensor network routing protocol [2] by Parno, Luk, Gaustad, and Perrig "PLGP" can be modified to provably resist Vampire attacks during the packet forwarding phase. The original version of the protocol, although designed for security, is vulnerable to Vampire attacks. 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. Here a modification in the forwarding phase of PLGP to provably avoid the above- mentioned attacks. First check 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: No-backtracking is satisfied if every packet p traverses the same number of hops whether or not an adversary is present in the network. To preserve no-backtracking, need to add a verifiable path history to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any significant adversarial influence on the path taken by any packet which traverses at least one honest node. Whenever a node n forwards packet p, this by attaching a non- repayable attestation (signature). These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node verifies the attestation chain to ensure that the packet has never travelled away from its destination in the logical address space.

System Architecture



VI. 1Valuable Secure Protocol Against Vampire Attacks

This section shows that the modification of clean slate secure sensor routing protocol [12] is provable security against vampire attack. The real version of this protocol is designed for security but it is

ISSN 2321-6905
JULY - 2015

Vulnerable to vampire attacks. A new valuable secure protocol (VSP) is proposed to prevent vampire attacks consists of following phases.

A. Network Configuring Phase

A network describes a collection of nodes and the links between them. The neighbor group formation process is done by each and every node in the network. This is the process of calculate the neighbor node value and find surrounding node. The neighbor list is maintained by all of nodes in the network. This process constructs a neighbor relationship tree and group membership that will used for addressing and routing. At the end of this process, each node learns every other node's virtual address, public key, and certificate, since every group members knows the identities of all other group members and the network converges to a single group Each and every node has initial energy value by it creation time. Every new nodes need to be authenticated before being allowed to join the WSN.

B. Key Management

This key management process is used for cryptography application during data transfer. Nodes generate a key to communicate with nodes in a group. Generated Key is established to all other nodes in a group. Every packet is encrypted and forwarded along the route. The cryptography technique used to protect the node and data from different kind of attacks. Elliptic curve cryptography (ECC) is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Compared with the other cryptography, ECC offers a better performance because it can achieve the same security with a smaller key size. It will minimize the number of calculation as well as save the time for nodes. Communication takes place independently by each node in a group.

C. Communication Phase

Communication across a network is performed by secure routing protocol is PLGP In PLGP node cannot able to determine the route to promote the packet. This makes malicious nodes to redirect the packets to any part of the network even if that distance is logically further away from the destination. The same data packets transmitting through the same node repeatedly to deplete the batteries quickly and leads to network death because of vampire. No-backtracking property is introduced to overcome this problem. It implies that for each packet in the protocol execution trace, the number of in-between honest nodes traversed by the packet between source and target is self-determining action of malicious nodes. The malicious node cannot perform carousel or stretch attack. Intelligent adversary may still influence packet progress. To prevent this situation by independently checking on packet movement to the Destination. In non source routing protocol packet routes are controlled by neighbor relationship and routing tree. Every node holds an identical copy of the address tree, and can verify the next logical hop. But this is not sufficient for backtracking. Function Secure packet forward(p) s- get source address (p); a–attestation (p); if(source sig is not verified (p)) or (empty (a) and not is neighbor (s)) then drop(p); for each node in a a do previous node – node; if (not are neighbors (node , previous node)) or (not making progress (previous node, node)) then - drop(p); c – nearest next node (s); p' – add (p); if is neighbor (c) then send (p',c); else forward (p',next hop to non neighbor (c)); To protect no- backtracking, add a certifiable path history to every PLGP packet. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any malicious influence on the path taken by any packet which traverses influence on the path taken by any packet which traverses at least one honest node. Every node in a network maintains a neighbor list. The resulting protocol, PLGP with attestations (PLGPa) uses this packet history together with PLGP's tree routing structure so every node can securely verify progress, preventing any malicious influence on the path taken by any packet which traverses at least one honest node. Whenever node n forwards packet p, by attaching a signature which cannot be modified by any node. These signatures form a chain attached to every packet, allowing any node receiving it to validate its path. Every forwarding node validates the attestation chain to ensure that the packet has never traveled away from its destination in the logical address space.

VII. Conclusions And Future Scope

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 implementations, but rather expose vulnerabilities in a number of popular protocol classes. We showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly generated topology of 30 nodes Theoretical worst case energy usage can increase by as much as a factor of O(N) per adversary per packet, where N is the network size. Authors proposed defenses against some of the forwarding-phase attacks and described PLGP-a, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. Authors have not offered a fully satisfactory solution for Vampire attacks

ISSN 2321-6905
JULY - 2015

during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGP-a. As WSN's become more and more crucial to everyday life availability faults become less tolerable. Thus high availability of these nodes is critical and must hold even under malicious condition.

References

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

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

[3] Gergely Acs, Levente Buttyan, and Istvan Vajda, Provably secure on demand source routing in mobile ad hoc networks, IEEE Transactions on mobile computing 05(2006),no.11.

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

[5] Daniel Bernstein and Peter Schwabe, New AES software speed records, INDOCRYPT, 2008.

[6] INSENS: Intrusion-tolerant routing for wireless sensor networks, Computer Communications 29 (2006), no. 2.

[7] Daniele Raffo, C´edric Adjih, Thomas Clausen, and Paul Muhlethaler, An advanced signature system for OLSR, SASN, 2004.

[8] John R. Douceur, The Sybil attack, International workshop on peer-topper systems, 2002.

[9] Computing, Lakshminarayanan Subramanian, Randy H. Katz, Volker Roth, Scott Shenker, and Ion Stoical, Reliable broadcast in unknown fixed- identity networks, Annual ACM SIGACT-SIGOPS symposium on principles of distributed 2005.

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

[11] Bryan Parno, Mark Luk, Evan Gaustad, and Adrian Perrig, Secure sensor network routing: A clean slate approach, Co NEXT, 2006.

[12] John R. Douceur, The Sybil attack, International workshop on peer-to peer systems, 2002.

[13] Thomas H. Clausen and Philippe Jacquet, Optimized link state routing protocol (OLSR), 2003.

[14] Charles E. Perkins and Pravin Bhagwat, Highly dynamic destination sequenced distance- vector routing (DSDV).

Authors:

Kantheti Bhanu Prakash received B.Tech from QIS College of Engineering and Technology, Ongole, from JNTU Kakinada, A.P, India. Presently , He was pursuing M.Tech in C.S.E from Bapatla Engineering College the specialization in Computer Science & Engineering. He presently pursuing M.Tech in Bapatla Engineering College, Bapatla, from Acharya Nagarjuna University, A.P, India.

Kumararaja Jetti received B.Tech in C.S.E from Bapatla Engineering College, from Acharya Nagarjuna University, A.P., India. M.Tech in C.S.E from BVC Engineering College, Odalarevu, from JNTU Kakinada, A.P., India. He has published papers in international journals and national conferences in the area of Network Security, Data Mining and Cloud Computing and is currently working as Assistant Professor in Dept of CSE, Bapatla Engineering College, Bapatla, A.P., India.