International Journal of Scientific Engineering and Applied Science (IJSEAS) - Volume-1, Issue-4, July 2015
ISSN: 2395-3470
www.ijseas.com

Enduring and Securing Network Node's Life using PLGP

S.J.Subhashini[1], **K.Nagalakshmi**[2], **M.Kumudha**[3], **K.R.Rincy**[4]
K.L.N College of Information Technology, Pottapalayam, India

Abstract

Ad hoc low-power wireless networks are an exciting research direction in sensing and pervasive computing. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. This paper explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining node's battery power. These "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. We find that all examined protocols are susceptible to Vampire attacks, which are devastating, difficult to detect, and are easy to carry out using as few as one malicious insider sending only protocol-compliant messages. In the worst case, a single Vampire can increase network-wide energy usage by a factor of O (N), where N in the number of network nodes. We discuss methods to mitigate these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

Index Terms: *Routing protocols, pervasive computing, Vampire attacks.*

1. Introduction

1.1 Secure Computing

Computer security (Also known as cyber security or IT Security) is information security is applied to computers and networks. The field covers all the processes and mechanisms by which computer-based equipment, information and services are protected from unintended or unauthorized access, change or destruction. Computer security also includes protection from unplanned events and natural disasters. Otherwise, in the computer industry, the term computer security refers to techniques for ensuring that data stored in the computer cannot be read or compromised by any individuals without authorization. Most computer security measures involve data encryption and passwords. Data encryption is the translation of data into a form that is unintelligible without a deciphering mechanism. A password is a secret word or phrase that gives a user access to a particular program or system.

1.2 Working conditions and basic needs in the secure computing

If we don't take basic steps to protect our work computer, we put it and all the information on it at risk. We can potentially compromise the operation of other computers on our organization's network, or even the functioning of the network as a whole.

A Physical security

Technical measures like login passwords, anti-virus are essential. However, a secure physical space is the first and more important line of defence. Is the place we keep our workplace computer secure enough to prevent theft or access to it while we are away? While the Security Department provides coverage across the Medical centre, it only takes seconds to steal a computer, particularly a portable device like a laptop or a PDA. A computer should be secured like any other valuable possession when we are not present. Human threats are not the only concern. Computers can be compromised by environmental mishaps (e.g., water, coffee) or physical trauma. Make sure the physical location of our computer takes account of those risks as well.

B Access passwords

The University's networks and shared information systems are protected in part by login credentials (user-IDs and passwords). Access passwords are also an essential protection for personal computers in most circumstances. Offices are usually open and shared spaces, so physical access to computers cannot be completely controlled. To protect our computer, we should consider setting passwords for particularly sensitive applications resident on the computer (e.g., data analysis software), if the software provides that capability.

C Prying eye protection

Because we deal with all facets of clinical, research, educational and administrative data here on the medical campus, it is important to do everything possible to minimize exposure of data to unauthorized individuals.

D Anti-virus software

Up-to-date, properly configured anti-virus software is essential. While we have server-side anti-virus software on our network computers, we still need it on the client side (our computer).

E Firewalls

Anti-virus products inspect files on our computer and in email. Firewall software and hardware monitor communications between our computer and the outside world. That is essential for any networked computer.

F Software updates

It is critical to keep software up to date, especially the operating system, anti-virus and anti-spyware, email and browser software. The newest versions will contain fixes for discovered vulnerabilities. Almost all anti-virus have automatic update features (including SAV). Keeping the "signatures" (digital patterns) of malicious software detectors up-to-date is essential for these products to be effective.

G Keep secure backups

Even if we take all these security steps, bad things can still happen. Be prepared for the worst by making backup copies of critical data, and keeping those backup copies in a separate, secure location. For example, use supplemental hard drives, CDs/DVDs, or flash drives to store critical, hard-to-replace data.

H Report problems

If we believe that our computer or any data on it has been compromised, our should make a information security incident report. That is required by University policy for all data on our systems, and legally required for health, education, financial and any other kind of record containing identifiable personal information. Ad-hoc wireless sensor networks (WSNs) promise instantly-deployable communication. “Vampire” attacks drain the life from networks nodes. In This project explores resource depletion attacks at the routing protocol layer. This system is intended to be a fully functioning network based database system. It will prevent the nodes from Vampire attacks. And increase the battery power by Clean-state sensor routing and three major contributions. For avoiding the vampire attacks and save the battery power using Clean Slate Sensor Routing By Parno et al, Luk ,Gaustad and Perrig which is also called as PLGP Protocol.

2. Related Work

In paper [1] is the most important step in software development process. Before developing the tool it is necessary to determine the time factor, economy and company strength. Once these things are satisfied, then next step is to determine which operating system and language can be used for developing the tool. This support can be obtained from senior programmers, from book or from websites. Before building the system the above consideration are taken into account for developing the proposed system.

In reference [2] identifies the necessary features of an on-demand minimum energy routing protocol and suggests mechanisms for their implementation. They 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. The authors have compared 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. The discussed the implementation of Dynamic Source Routing (DSR) protocol using the Click modular router on a real life test-bed consisting of laptops and wireless Ethernet cards. Finally, describe the modifications made to the DSR router to make it energy aware.

In reference[3] 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 (Path-based Denial of Service). In a PDoS attack, an adversary overwhelms sensor nodes a long distance away by flooding a multihop end-to-end communication path with either replayed packets or injected spurious packets. This paper proposes a solution using one-way hash chains to protect end-to-end communications in WSNs against PDoS attacks. The proposed solution is lightweight, tolerates bursty packet losses, and can easily be implemented in modern WSNs. The paper reports on performance measured from a prototype implementation.

In paper[4] describes an INtrusion-tolerant routing protocol for wireless SEnsor NetworkS (INSENS). INSENS securely and efficiently constructs tree-structured routing for wireless sensor networks (WSNs). The key objective of an INSENS network is to tolerate damage caused by an intruder who has compromised deployed sensor nodes and is intent on injecting, modifying, or blocking packets. To limit or localize the damage caused by such an intruder, INSENS incorporates distributed lightweight security mechanisms, including efficient one-way hash chains and nested keyed message authentication codes that defend against wormhole attacks, as well as multipath routing. Adapting to WSN characteristics, the design of INSENS also pushes complexity away from resource-poor sensor nodes towards resource-rich base stations. An enhanced single-phase version of INSENS scales to large networks, integrates bidirectional verification to defend against rushing attacks, accommodates multipath routing to multiple base stations, enables secure joining/leaving, and incorporates a novel pair wise key setup scheme based on transitory global keys that is more resilient than LEAP. Simulation results are presented to demonstrate and assess the tolerance of INSENS to various attacks launched by an adversary. A prototype implementation of INSENS over a network of MICA2 motes is presented to evaluate the cost incurred.[4]Routing is one of the most basic networking functions in mobile ad hoc networks. Hence, an adversary can easily paralyze the operation of the network by attacking the routing protocol. This has been realized by many researchers and several "secure" routing protocols have been proposed for ad hoc networks. However, the security of those protocols has mainly been analyzed by informal means only. In this paper, we argue that flaws in ad hoc routing protocols can be very subtle, and we advocate a more systematic way of analysis. We propose a mathematical framework in which security can be precisely defined and routing protocols for mobile ad hoc networks can be proved to be secure in a rigorous manner. Our framework is tailored for on-demand source routing protocols, but the general principles are applicable to other types of protocols too. Our approach is based on the simulation paradigm, which has already been used extensively for the analysis of key establishment protocols, but, to the best of our knowledge, it has not been applied in the context of ad hoc routing so far. We also propose a new on-demand source routing protocol, called endairA, and we demonstrate the use of our framework by proving that it is secure in our model

In this paper[5], they have considered routing security in wireless sensor networks. Many sensor network routing protocols have been proposed, but none of them have been designed with security as a goal. They proposed security goals for routing in sensor networks, show how attacks against ad-hoc and peer-to-peer networks can be adapted into powerful attacks against sensor networks, introduce two classes of novel attacks against sensor networks sinkholes and HELLO floods, and analyze the security of the entire major sensor network routing protocols. They described crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.

3. System Design

It is a simple graphical formalism that can be used to represent a system in terms of the input data to the system, various processing carried out on these data, and the output data is generated by the system.

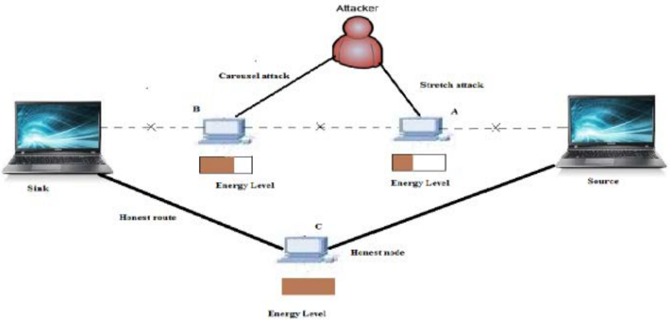

Fig 3.1 Architecture diagram

4. Proposed Work

We setup our Network model with Sink, Source and with Six nodes namely Node A, B, C, D, E, F. Each node will be assigned unique Identity number. And also where topology discovery is done at transmission time, and static protocols, where topology is discovered during an initial setup phase, with periodic rediscovery to handle rare topology changes. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Furthermore, adversary location within the network is assumed to be fixed and random, as if an adversary corrupts a number of honest nodes before the network was deployed, and cannot control their final positions.

A Carousel Attack

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 the figure. 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 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

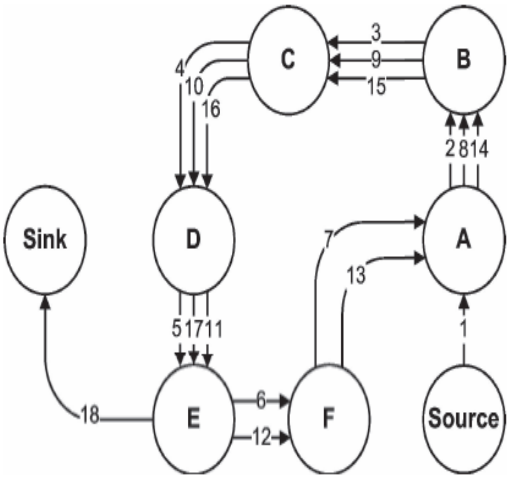

Fig 4.1 Carousel Attack

B Stretch Attack

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. 1b. 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 overheard packets, we assume that only messages originated by adversaries may have maliciously composed routes.

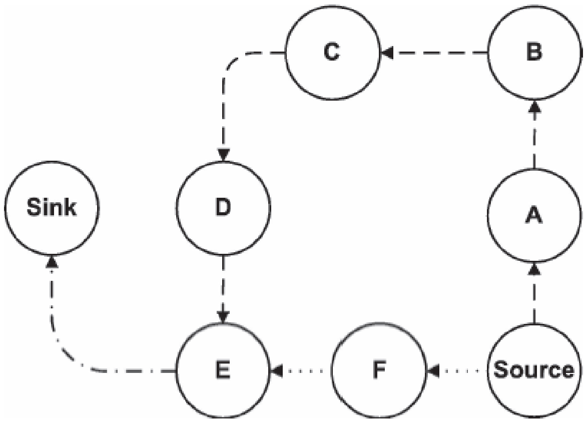

Fig 4.2 Stretch Attack

C Energy level Identification

In this module, we show the energy level identification of each nodes to show the vampire attack reactions. A node is permanently disabled once its battery power is exhausted; let us briefly consider nodes that recharge their batteries in the field, using either continuous charging or switching between active and recharge cycles. In the continuous charging case, power-draining attacks would be effective only if the adversary is able to consume power at least as fast as nodes can recharge. Assuming that packet processing drains at least as much energy from the victims as from the attacker, a continuously recharging adversary can keep at least one node permanently disabled at the cost of its own functionality. However, recall that sending any packet automatically constitutes amplification, allowing few Vampires to attack many honest nodes.

D Secured Transmission

In this module, we show the secured transmission done in the nodes by overcoming the vampire attacks. Where the data travels in the honest route and mitigating the vampire attacks and which also saves the node's energy level as high.

4. Implementation

PLGP is a clean-slate secure sensor network routing protocol by Parno et al. Discovery deterministically organizes nodes into a tree that will later be used as an addressing scheme. 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 neighbours using local broadcast, and form ever expanding "neighbourhoods", stopping when the entire network is a single group. Throughout this process, nodes build a tree of neighbour relationships and group membership that will later be used for addressing and routing.

PLGP consists of

- Topology discovery phase.
- Forming groups and addressing.
- Packet forwarding phase.

A Topology discovery phase

At the point 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.

B Forming groups and addressing

Each node starts as its own group of size one, with a virtual address 0. Nodes who overhear presence broadcasts form groups with their neighbours. When two individual nodes (each with an initial address 0) form a group of size two, one of them takes the address 0, and the other becomes 1. Like individual nodes, each group will initially choose a group address 0,and will choose 0 or 1 when merging with another group. Each group member appends the group address to their own address, e.g., node 0 in group 0 becomes 0.0, and node 0 in group 1 becomes 1.0, and so on. Each time two groups merge, the address of each node is lengthened by 1 bit. Implicitly, this forms a binary tree of all addresses in the network, with node addresses as leaved. When larger groups merge, they both broadcast their group IDs (and the IDs of all group members) to each other, and proceed with a merge protocol identical to the two-node case. Groups that have grown large enough that some members are not within radio range of other groups will communicate through "gateway nodes" ,which are within range of both groups. Every node within a group will end up with a next-hop path to every other group, as in distance vector. Topology discovery proceeds in this manner until all network nodes are members of a single group. By the end of topology discovery, 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.

C Packet forwarding

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. In PLGP, forwarding nodes do not know what path a packet took, allowing adversaries to divert packets to any part of the network, even if that area is logically further away from the destination than the malicious node. This makes PLGP vulnerable to Vampire attacks. An honest node has no way to tell that the packet it just received is moving away from the destination; the only information available to the honest node is its own address and the packet destination address.

5. Conclusion and Future Work

In this paper, we defined 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. 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. 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. Theoretical worst case energy usage can increase by as much as a factor adversary per packet, where N is the network size. We proposed defenses against some of the forwarding-phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGPa. Derivation of damage bounds and for topology discovery, as well as handling mobile networks, is left for future work.

References

[1] Secure Routing In Wireless Sensor Networks Attacks and Counter
measures Authors : C. Karlof and D. Wagner

[2] D.Bernstein and P. Schwabe, "New AES Software Speed Records,"Proc. Ninth Int'l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[3]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.

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

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

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

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

[8] B. Mukherjee, L.T. Heberlein, and K.N. Levitt, "Network IntrusionDetection," IEEE Network, vol. 8, no. 3, pp. 26-41, May 1994.

[9] P. Garcı´a-Teodoro, J. Dı´az-Verdejo, G. Macia´-Ferna´ndez, and E.Va´zquez, "Anomaly-Based Network Intrusion Detection: Techniques,Systems and Challenges," Computers and Security, vol. 28,nos. 1/2, pp. 18-28, Feb./Mar 2009.

[10] A. Jones and S. Li, "Temporal Signatures for Intrusion Detection,"Proc. 17th Ann. Computer Security Applications Conf. (ACSAC),pp. 252-261, Dec. 2001.

[11] L. Wang, A. Liu, and S. Jajodia, "Using Attack Graphs forCorrelating, Hypothesizing, and Predicting Intrusion Alerts,"Computer Comm., vol. 29, no. 15, pp. 2917-2933, Sept. 2006.

[12] S. Noel, E. Robertson, and S. Jajodia, "Correlating Intrusion Eventsand Building Attack Scenarios through Attack Graph Distances,"Proc. Ann. Computer Security Applications Conf. (ACSAC), pp. 350-359, Dec. 2004.

[13] H. Debar and A. Wespi, "Aggregation and Correlation ofIntrusion-Detection Alerts," Proc. Fourth Int'l Symp. RecentAdvances in Intrusion Detection (RAID), pp. 85-103, Oct. 2001.