Wireless Secured Ad-Hoc Sensor Network to Overcome Vampire Attack

David R B J,
Department of ECE,
SCAD Engineering College
Tirunelveli

Deivabalasubramanian S,
Department of ECE,
SCAD Engineering college
Tirunelveli

Sakthi Chidambaram @ Aravind J,
Department of ECE,
SCAD Engineering college
Tirunelveli

Davidraja D,
Department of ECE,
SCAD Engineering college
Tirunelveli

***Abstract*-Ubiquitous on-demand computing power, continuous connectivity, and instantly deployable communication for military and first responders are some of the exciting applications for future technology which securely works in wireless ad hoc Networks. Direction in sensing and pervasive computing are the basic process in which wireless networks works. wireless ad hoc networks are particularly vulnerable to denial of service (DoS) attacks , and a great deal of research has been done to enhance survivability. Prior security work in this area has focused primarily on denial of communication at the routing or medium access control levels. We consider how routing protocols, even those designed to be secure, lack protection from these attacks, which we call Vampire attacks, since they drain the life from networks nodes. 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. Mitigating these types of attacks, including a new proof-of-concept protocol that provably bounds the damage caused by Vampires during the packet forwarding phase is introduced in this work.**

Index Terms—Denial of service, security, routing, ad hoc networks, sensor networks, wireless networks

I. INTRODUCTION:

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. As WSNs become more and more crucial to the everyday functioning of people and organizations, availability faults become less tolerable lack of availability can make the difference between business as usual and lost productivity, power outages, environmental disasters, and even lost lives; thus high availability of these networks is a critical property, and should hold even under malicious conditions. One such DOS attack is Vampire attack-Draining of node life from wireless ad-hoc sensor networks.

Vampire attack means creating and sending messages by malicious node which causes more energy consumption by the network leading to slow depletion of node's battery life. This attack is not specific to any protocol. Few kinds of attacks are carousal and stretch attack, since they drain the life from networks nodes. These attacks are distinct from previously studied DoS, reduction of quality (RoQ), and routing infrastructure attacks as they do not disrupt immediate availability, but rather work over time to entirely disable a network. While some of the individual attacks are simple, and power draining and resource exhaustion attacks have been discussed before, prior work has been mostly confined to other levels of the protocol stack, e.g., medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks.

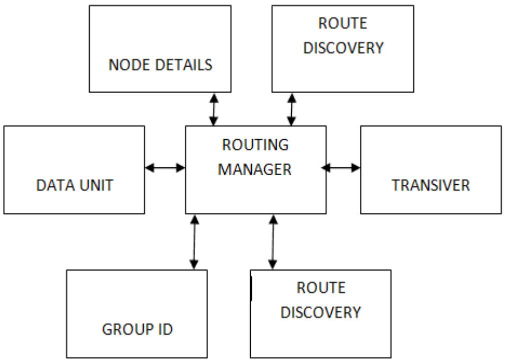
Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing Infrastructure. Vampires do not disrupt or alter discovered paths, instead using existing valid network paths and protocol-compliant messages. Protocols that maximize power efficiency are also inappropriate, since they rely on cooperative node behavior and cannot optimize out malicious action. We modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

II. PROBLEM DEFINITION

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. Our adversaries are malicious insiders and have the same resources and level of network access as honest nodes. Intelligent adversary placement or dynamic node compromise would make attacks far more damaging. Even in non-power-constrained systems, depletion of resources such as memory, CPU time, and bandwidth may easily cause problems. Malicious intermediaries using intelligent packet dropping strategies can significantly degrade performance of TCP streams traversing those nodes.

III. BLOCK DIAGRAM



IV. EXISTING SYSTEM:

While some of the individual attacks are simple, and power draining and resource exhaustion attacks have been discussed before prior work has been mostly confined to other levels of the protocol stack, e.g., medium access control (MAC) or application layers, and to our knowledge there is little discussion, and no thorough analysis or mitigation, of routing-layer resource exhaustion attacks. A very early mention of power exhaustion can be found, as "sleep deprivation torture." As per the name, the proposed attack prevents nodes from entering a low-power sleep cycle, and thus deplete 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.

Disadvantages: Excess load on legitimate nodes.Do not use or return illegal routes or prevent communication in the short term.

Modules:

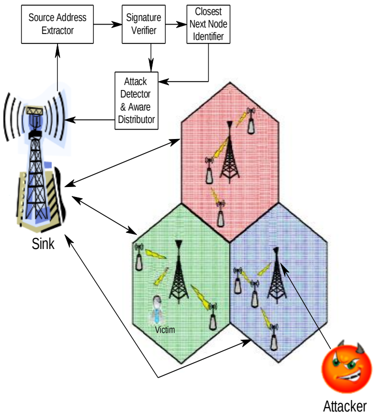
*Adversaries and Honest node Module:*All routing protocols employ at least one topology discovery period, since ad hoc deployment implies no prior position knowledge. Limiting ourselves to immutable but dynamically organized topologies, as in most wireless sensor networks, we further differentiate on-demand routing protocols, 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. Vampire in terms of the "maliciousness" of the adversary, or the induced stretch of the optimal route in number of hops. This reduces cumulative network energy, or almost the entire lifetime of a single node. Therefore, the stretch attack increases the effectiveness of an adversary by an order of magnitude, reducing its energy expenditure to compose and transmit messages. Forwarding nodes using minimum-energy routing could replace long distance transmissions with a number of shorter distance hops, but the attack still works since the malicious path is longer. Rate limiting also potentially punishes honest nodes that may transmit large amounts of time-critical (bursty) data.

*Loop detection Module:*One of the attractive features of source routing is that the route can it is better to simply drop the packet, especially considering that the sending node is likely malicious (honest nodes should not introduce loops). The described attacks are only valid within the network "neighborhood" of the adversarial node. An alternate solution is to alter how intermediate nodes process the source route. To forward a message, a node must determine the next hop by locating itself in the source route. If a node searches for itself from the destination backward instead from the source forward, any loop that includes the current node will be automatically truncated (the last instance of the local node will be found in the source route rather than the first). No extra processing is required for this defense, since a node must perform this check anyway, we only alter the way the check is done.

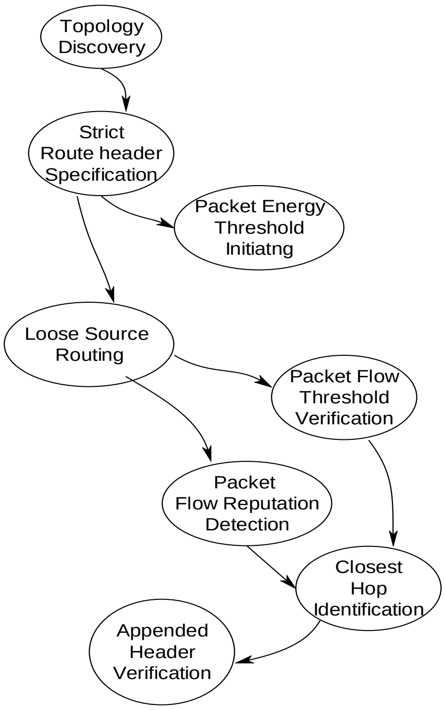
*Loose Source Routing:*We can define loose source routing, where intermediate nodes may replace part or all of the route in the packet header if they know of a better route to the destination. This makes it necessary for nodes to discover and cache optimal routes to at least some fraction of other nodes, partially defeating the as-needed discovery advantage. Caching must be done carefully lest a maliciously suboptimal route be introduced.

*No-backtracking:*Routes are dynamically composed of forwarding decisions made independently by each node. PLGP differs from other protocols in that packets paths are further bounded by a tree, forwarding packets along the shortest route through the tree that is allowed by the physical topology. 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.

V. ARCHITECTURE DIAGRAM:


Source Address Extractor
Signature Verifier
Closest Next Node Identifier
Attack Detector & Aware Distributor
Sink
Victim
Attacker

VI. DATA FLOW DIAGRAM:


Topology Discovery
Strict Route header Specification
Packet Energy Threshold Initiatng
Loose Source Routing
Packet Flow Threshold Verification
Packet Flow Reputation Detection
Closest Hop Identification
Appended Header Verification

Power-aware localized routing in wireless networks

We discuss routing algorithms for wireless networks with the goal of increasing the network and node life. Recently, a cost aware metric based on remaining battery power at nodes was proposed and verified for non-localized shortest-cost routing algorithms, assuming constant transmission power. Two metrics where transmission power depends on distance between nodes were also recently proposed. We define a new power-cost metric based on the combination of both node's lifetime and distance based power metrics. We then propose power, cost, and power-cost GPS based fully distributed (i.e. localized) routing algorithms, where nodes make routing decisions solely on the basis of location of their neighbors and destination. Power aware localized routing algorithm attempts to minimize the total power needed to route a message between a source and a destination. Cost-aware localized algorithm is aimed at extending battery's worst case lifetime. The combined power-cost localized routing algorithm attempts to minimize the total power needed and to avoid nodes with short battery's remaining lifetime. We prove that the proposed localized power, cost, and power-costefficient routing algorithms are loop-free, and show their efficiency by experiments.

Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures

We consider 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. We propose 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 all the major sensor network routing protocols. We describe crippling attacks against all of them and suggest countermeasures and design considerations. This is the first such analysis of secure routing in sensor networks.

An On-demand Minimum Energy Routing Protocol for a Wireless Ad Hoc Network

A minimum energy routing protocol reduces the energy consumption of the nodes in a wireless ad hoc network by routing packets on routes that consume the minimum amount of energy to get the packets to their destination. This paper identifies the necessary features of an on-demand minimum energy routing protocol and suggests mechanisms for their implementation. We highlight 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. We compare 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. We discuss 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 we describe the modifications we have made to the DSR router to make it energy aware.

Energy Efficiency of QoS Routing in Multi-Hop Wireless Networks

The trend of adopting more and more wireless mobile computers and smartphones has changed our way of living. Those devices heavily rely on the underlying wireless network systems to provide adequate communication support. As streaming audio and video becomes norm, the requests for stringent maximum end-to-end latency and minimum bandwidth make the networking process more difficult. Quality of Service (QoS) routing is designed to fulfill such requirements. In this paper, we study the performance of QoS routing in multi-hop wireless networks from the perspective of energy efficiency. Since there are sophisticated relationships between wireless radio propagation and energy consumption, various QoS routing strategies produce significantly different results in terms of energy efficiency. Through extensive simulation experiments, the shortest path routing, minimum energy routing, minimum hop routing, and maximum throughput routing are compared.

Energy Efficient Method for Detection and Prevention of False Reports in Wireless Sensor Networks

In a wireless sensor network, various attacks such as the false injection attack, easily occur by malicious attackers. This attack drains the finite energy resources of each node to destroy functions of the sensor network. SEF (statistical en-route filtering scheme) was proposed to probabilistically detect the false reports in intermediate nodes while forwarding processes. In this paper, we propose a security method which uses three types of keys and a black list to prepare a countermeasure against the false report injection attack. Three types of keys are used in each node - an individual key for encrypting event information between a node and a base station, a pairwise key for maintaining secure routing paths between the intermediate nodes, and a cluster key for detecting forged MACs between the neighboring nodes of a cluster region. A center-of-stimulus node prevents forged MACs through the black list while they consistently occur from the compromised node. SEF is evaluated with the proposed method, for efficient energy consumption of each node. The experiment results show that our proposed method enhances energy savings more compared to the SEF in the sensor network.

Energy-efficient Itinerary Planning for Mobile Agents in Wireless Sensor Networks

Compared to conventional wireless sensor networks (WSNs) that are operated based on the client-server computing model, mobile agent (MA) systems provide new capabilities for energy-efficient data dissemination by flexibly planning its itinerary for facilitating agent based data collection and aggregation. It has been known that finding the optimal itinerary is NP-hard and is still an open area of research. In this paper, we consider the impact of both data aggregation and energyefficiency in sensor networks itinerary selection, We propose an *itinerary energy minimum for first-source-selection* (IEMF) algorithm, as well as the *itinerary energy minimum algorithm* (IEMA), the iterative version of IEMF. Our simulation experiments show that IEMF provides higher energy efficiency and lower delay compared to existing solutions, and IEMA outperforms IEMF with some moderate increase in computation complexity.

Mobile Base Stations Placement and Energy Aware Routing in Wireless Sensor Networks

Increasing network lifetime is important in wireless sensor/ad-hoc networks. In this paper, we are concerned with algorithms to increase network lifetime and amount of data delivered during the lifetime by deploying multiple mobile base stations in the sensor network field. Specifically, we allow multiple mobile base stations to be deployed along the periphery of the sensor network field and develop algorithms to dynamically choose the locations of these base stations so as to improve network lifetime. We propose energy efficient low-complexity algorithms to determine the locations of the base stations; they include *i*) Top-*Kmax* algorithm, *ii*) maximizing the minimum residual energy (Max-Min-RE) algorithm, and *iii*) minimizing the residual energy difference (MinDiff-RE) algorithm. We show that the proposed base stations placement algorithms provide increased network lifetimes and amount of data delivered during the network lifetime compared to single base station scenario as well as multiple static base stations scenario, and close to those obtained by solving an integer linear program (ILP) to determine the locations of the mobile base stations. We also investigate the lifetime gain when an energy aware routing protocol is employed along with multiple base stations.

Providing End-to-End Secure Communications in Wireless Sensor Networks

In many Wireless Sensor Networks (WSNs), providing end to end secure communications between sensors and the sink is important for secure network management. While there have been many works devoted to hop by hop secure communications, the issue of end to end secure communications is largely ignored. In this paper, we design an end to end secure communication protocol in randomly deployed WSNs. Specifically, our protocol is based on a methodology called differentiated key pre-distribution. The core idea is to distribute different number of keys to different sensors to enhance the resilience of certain links. This feature is leveraged during routing, where nodes route through those links with higher resilience. Using rigorous theoretical analysis, we derive an expression for the quality of end to end secure communications, and use it to determine optimum protocol parameters. Extensive performance evaluation illustrates that our solutions can provide highly secure communications between sensor nodes and the sink in randomly deployed WSNs. We also provide detailed discussion on a potential attack (i.e. biased node capturing attack) to our .solutions, and propose several countermeasures to this attack.

Stealthy Attacks in Wireless Ad Hoc Networks: Detection and Countermeasure.

Stealthy packet dropping is a suite of four attacks—misrouting, power control, identity delegation, and colluding collision—that can be easily launched against multihop wireless ad hoc networks. Stealthy packet dropping disrupts the packet from reaching the destination through malicious behavior at an intermediate node.

However, the malicious node gives the impression to its neighbors that it performs the legitimate forwarding action. Moreover, a legitimate node comes under suspicion. A popular method for detecting attacks in wireless networks is behavior-based detection performed by normal network nodes through overhearing the communication in their neighborhood. This leverages the open broadcast nature of wireless communication. An instantiation of this technology is local monitoring. We show that local monitoring, and the wider class of overhearing-based detection, cannot detect stealthy packet dropping attacks. Additionally, it mistakenly detects and isolates a legitimate node. We present a protocol called SADEC that can detect and isolate stealthy packet dropping attack efficiently. SADEC presents two techniques that can be overlaid on baseline local monitoring: having the neighbors maintain additional information about the routing path, and adding some checking responsibility to each neighbor. Additionally, SADEC provides an innovative mechanism to better utilize local monitoring by considerably increasing the number of nodes in a neighborhood that can do monitoring.

Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks

As mobile ad hoc network applications are deployed, security emerges as a central requirement. In this paper, we introduce the *wormhole attack*, a severe attack in ad hoc networks that is particularly challenging to defend against. The wormhole attack is possible even if the attacker has not compromised any hosts, and even if all communication provides authenticity and confidentiality. In the wormhole attack, an attacker records packets (or bits) at one location in the network, tunnels them to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks, especially against many ad hoc network routing protocols and location-based wireless security systems. For example, most existing ad hoc network routing protocols, without some mechanism to defend against the wormhole attack, would be unable to and routes longer than one or two hops, severely disrupting communication

VII. PROPOSED SYSTEM:

We made three primary contributions. First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. We observe that security measures to prevent Vampire attacks are orthogonal to those used to protect routing infrastructure, and so existing secure routing protocols. We will assume *Department of ECE,* that 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.

Advantages:

Cannot optimize out malicious action like maximize power efficiency of network, which is inappropriate.

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

.

VIII. CONCLUSION

we defined Vampire attacks, a new class of resource consumption attacks that use routing protocols topermanently disable ad hoc wireless sensor networks bydepleting 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..

We proposed defenses against some of the forwarding-phase attacks and described PLGPa, the first sensor networkrouting protocol that provably bounds damage fromVampire attacks by verifying that packets consistentlymake 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 defenses for topology discovery, as well as handling mobile networks, is left for future work.

IX. REFERENCES:

1. C. Karlof and D. Wagner, "Secure Routing in Wireless Sensor Networks: Attacks and Countermeasures," Proc. IEEE Int'l workshop Sensor Network Protocols and Applications, 2003.
2. S. Doshi, S. Bhandare, and T.X. Brown, "An On-Demand Minimum Energy Routing Protocol for a Wireless Ad Hoc "Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.
3. Y.-C. Hu, D.B. Johnson, and A. Perrig, "SEAD: Secure Efficient Distance Vector Routing for Mobile Wireless Ad Hoc Networks," Proc. IEEE Workshop Mobile Computing Systems and Applications, 2002.
4. Y.-C. Hu, D.B. Johnson, and A. Perrig, "Ariadne: A Secure On-Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.
5. L.M. Feeney, "An Energy Consumption Model for Performance Analysis of Routing Protocols for Mobile Ad Hoc Networks," Mobile Networks and Applications, vol. 6, no. 3, pp. 239-249, 2001