Wireless Ad Hoc Sensor Networks Saturating in Draining Life

M. Lakshmi Madhuri[1] and Mr. S. Durga Prasad[2]

1. Final Year M.Tech, Department of CSE, Baba Institute of Technology and Sciences, Visakhapatnam, AP, India.
2. Associate Professor, Department of CSE, Baba Institute of Technology and Sciences Visakhapatnam, AP. India

Abstract: Adhoc sensor wireless networks have been drawing interest among the researchers in the direction sensing and pervasive computing. The security work in this area is priority and primarily focusing on denial of communication at the routing or medium access control levels. In this paper the attacks, which is mainly focusing on routing protocol, layer that kind of attacker is known as resource depletion attacks. This attacks causing the impact of persistently disabling the networks by drastically draining the node's battery power. These "Vampire" attacks are not impacting any specific kind of protocols. Finding of vampire attacks in the network is not an easy one. It's very difficult to detect, devastating .A simple vampire presenting in the network can increasing network wide energy usage. We discuss some methods and alternative routing protocols solution will be avoiding some sort of problems which causing by vampire attacks. 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 nodes' battery power. These "Vampire" attacks are not specific to any 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.
Keywords**:** *Networks; Wireless Networks; Adhoc Networks; Routing Protocols.*

Introduction:

A wireless ad hoc sensor network consists of a number of sensors spread across a geographical area. Each sensor has wireless communication capability and some level of intelligence for signal processing and networking of the data. Some examples of wireless ad hoc sensor networks are the following Military sensor networks to detect and gain as much information as possible about enemy movements, explosions, and other phenomena of interest. Sensor networks to detect and characterize Chemical, Biological, Radiological, Nuclear, and Explosive (CBRNE) attacks and material. Sensor networks to detect and monitor environmental changes in plains, forests, oceans, etc.

Wireless traffic sensor networks to monitor vehicle traffic on highways or in congested parts of a city. Wireless surveillance sensor networks for providing security in shopping malls, parking garages, and other facilities .Wireless parking lot sensor networks to determine which spots are occupied and which are free. The above list suggests that wireless ad hoc sensor networks offer certain capabilities and enhancements in operational efficiency in civilian applications as well as assist in the national effort to increase alertness to potential terrorist threats. Two ways to classify wireless ad hoc sensor networks are whether or not the nodes are individually addressable, and whether the data in the network is aggregated. The sensor nodes in a parking lot network should be individually addressable, so that

one can determine the locations of all the free spaces. This application shows that it may be necessary to broadcast a message to all the nodes in the network. If one wants to determine the temperature in a corner of a room, then addressability may not be so important. Any node in the given region can respond. The ability of the sensor network to aggregate the data collected can greatly reduce the number of messages that need to be transmitted across the network. This function of data fusion is discussed more below. The basic goals of a wireless ad hoc sensor network generally depend upon the application, but the following tasks are common to many networks. Determine the value of some parameter at a given location: In an environmental network, one might one to know the temperature, atmospheric pressure, amount of sunlight, and the relative humidity at a number of locations. This example shows that a given sensor node may be connected to different types of sensors, each with a different sampling rate and range of allowed values. Detect the occurrence of events of interest and estimate parameters of the detected event or events: In the traffic sensor network, one would like to detect a vehicle moving through an intersection and estimate the speed and direction of the vehicle. Classify a detected object: Is a vehicle in a traffic sensor network a car, a mini-van, a light truck, a bus, etc. Collaborative signal processing: Yet another factor that distinguishes these networks from MANETs is that the end goal is detection/estimation of some events of interest, and not just communications. To improve the detection/estimation performance, it is often quite useful to fuse data from multiple sensors. This data fusion requires the transmission of data and control messages, and so it may put constraints on the network architecture.

Querying ability:

A user may want to query an individual node or a group of nodes for information collected in the region. Depending on the amount of data fusion performed, it may not be feasible to transmit a large amount of the data across the network. Instead, various local sink nodes will collect the data from a given area and create summary messages. A query may be directed to the sink node nearest to the desired location.

Sensor types and system architecture:

With the coming availability of low cost, short range radios along with advances in wireless networking, it is expected that wireless ad hoc sensor networks will become commonly deployed. In these networks, each node may be equipped with a variety of sensors, such as acoustic, seismic, infrared, still/motion video camera, etc. These nodes may be organized in clusters such that a locally occurring event can be detected by most of, if not all, the nodes in a cluster. Each node may have sufficient processing power to make a decision, and it will be able to broadcast this decision to the other nodes in the cluster. One node may act as the cluster master, and it may also contain a longer range radio using a protocol such as IEEE 802.11 or Bluetooth.

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.

This paper makes 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 such as Ariadne SAODV [78], and SEAD [28] do not protect against Vampire attacks. Existing work on secure routing attempts to ensure that adversaries cannot cause path discovery to return an invalid network path, but 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. Second, we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary). Third, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

Availability ensures the survivability of network services despite denial of service attacks. A denial of service attack could be launched at any layer of an ad hoc network. On the physical and media access control layers, an adversary could employ jamming to interfere with communication on physical channels. On the network layer, an adversary could disrupt the routing protocol and disconnect the network. On the higher layers, an adversary could bring down high-level services. One such target is the key management service, an essential service for any security framework. Confidentiality ensures that certain information is never disclosed to unauthorized entities. Network transmission of sensitive information, such as strategic or tactical military information, requires confidentiality. Leakage of such information to enemies could have devastating consequences. Routing information must also remain confidential in certain cases, because the information might be valuable for enemies to identify and to locate their targets in a battlefield. Integrity guarantees that a message being transferred is never corrupted. A message could be corrupted because of benign failures, such as radio propagation impairment, or because of malicious attacks on the network. Authentication enables a node to ensure the identity of the peer node it is communicating with. Without authentication, an adversary could masquerade a node, thus gaining unauthorized access to resource and sensitive information and interfering with the operation of other nodes. Finally, non-repudiation ensures that the origin of a message cannot deny having sent the message. Non repudiation is useful for detection and isolation of compromised nodes. When a node A receives an erroneous message from a node B, non-repudiation allows A to accuse B using this message and to convince other nodes that B is compromised. There are other security goals (e.g., authorization) that are of concern to certain applications, but we will not pursue these issues in this paper.

Classification:

In this paper, the use of low-power wireless sensor networks for the classification of signals is described. The objective is to accurately classify the target signals using a novel decentralized approach that aims to reduce the energy consumption of the network nodes as much as possible. Since, often, the most consuming part of such nodes is the radio module, the proposed

solution performs the classification of the selected features of a detected signal directly on the board, thus transmitting only the classification results. As a case study, the identification of vehicles that emit acoustic signals is considered. For this case, the process of feature extraction and selection is based on a spectral analysis of the signals, whereas the classification is carried out by support vector machines, which were chosen for their flexibility in classifying patterns. In particular, the use of the -SVM classification algorithm is proposed because it is expected to provide a good performance in terms of both implementation cost and classification accuracy. Finally, the advantages of the proposed solution in terms of energy consumption are illustrated with reference to an implementation based on the Mica2 sensor node by Crossbow Technology Inc.

Properties of Ad Hoc Networks:

Ad hoc networks have become a major research domain during the last decade. This trend is mainly forced by recent advances in microelectronics and wireless communications. Engineers have been enabled to develop a new generation of communication devices. Depending on the application scenario, different requirements have to be considered (see below). All these applications have some common properties: the interconnected devices have to form a network in an ad hoc manner, i.e. spontaneously, have to maintain the network state and coordinate the information exchange. In some scenarios, the overall goal is pre-deployed in all single devices while others are mainly user-driven. The grade of interactivity greatly influences the possible solutions for controlling, i.e. organizing the network.

Ad hoc networks have various applications and characteristics, and are therefore categorized into sensor networks, mobile ad hoc networks, mobile sensor networks, and mesh networks in this paper. We investigate and analyze each category of ad hoc networks. The most important characteristics, challenges and open issues in each one are addressed and summarized. Applicable solutions to these issues are proposed and suggestions are made. The systematic analysis of ad hoc networks in this paper will allow the reader to better understand these networks so that one would be able to propose efficient and effective schemes to improve their performances.

Related Work:

Today, many people carry numerous portable devices, such as laptops, mobile phones, IPDAs and mp3 players, for use in their professional and private lives. For the most part, these devices are used separately—that is, their applications do not interact. Imagine, however, if they could interact directly: participants at a meeting could share documents or presentation. Business cards would automatically find their way into the address register on a laptop and the number register on a mobile phone; as commuters exit a train, their laptops could remain online; likewise, incoming email could now be diverted to their PDAs; finally, as they enter the office, all communication could automatically be routed through the wireless corporate campus network. These examples of spontaneous, ad hoc wireless communication between devices might be loosely defined as a scheme, often referred to as ad hoc networking, which allows devices to establish communication, anytime and anywhere without the aid of a central infrastructure. Actually, ad hoc networking as such is not new, but the setting, usage and players are. In the past, the notion of ad hoc networks was often associated with communication on combat fields and at the site of a disaster area; now, as novel technologies such as Bluetooth materialize, the

scenario of ad hoc networking is likely to change, as is its importance. In this article, the authors describe the concept of ad hoc networking by giving its background and presenting some of the technical challenges it poses. The authors also point out some of the applications that can be envisioned for ad hoc networking

Typical Applications:

Mobile ad hoc networks have been the focus of many recent research and development efforts. So far, ad hoc packet-radio networks have mainly been considered for military applications, where a decentralized network configuration is an operative advantage or even a necessity. In the commercial sector, equipment for wireless, mobile computing has not been available at a price attractive to large markets. However, as the capacity of mobile computers increases steadily, the need for unlimited networking is also expected to rise. Commercial ad hoc networks could be used in situations where no infrastructure (fixed or cellular) is available. Examples include rescue operations in remote areas, or when local coverage must be deployed quickly at a remote construction site. Ad hoc networking could also serve as wireless public access in urban areas, providing quick deployment and extended coverage. The access points in networks of this kind could serve as stationary radio relay stations that perform ad hoc routing among themselves and between user nodes. Some of the access points would also provide gateways via which users might connect to a fixed backbone network.

Making connections stateless:

We show how to make protocols stateless by passing the state information between the protocol principals along the messages. Add integrity check to the state data and to the entire connection. Compares the behavior of tasteful and stateless protocols under denial-of-service attacks.

Transformation from tasteful into stateless

Assuming that the communication channels are reliable and coding attacks the only concern, we can transform any tasteful client/server protocol or communication protocol with initiator and responder into a stateless equivalent. This is done by sending state information from the server to the client with every message. Along the next message from the client, the state information is returned to the server. A tasteful protocol and an equivalent stateless protocol.

Usually the server or the responding principal is the primary target of the denial-of-service threats and it is su-cient to make this principal stateless. In a symmetric protocol it is also possible to make both principals stateless by passing the states of both principals between them. Similar transformations are possible for multi-party protocols if the messages travel suitably. There one must take care that the state information is returned to the stateless principal in time. The main reason for the stateless transformation is that it makes the system behavior more ideal. When there is no limit on the number of clients, the limit cannot be exploited by denial-of-service attacks. The ideal protocol properties also simplify quantitative analysis of system behavior under stress. Moreover, the stateless protocol moves the responsibility of saving the state information from the server to the client. The client, who has requested the service, is better motivated to maintain the information and to recover from error conditions and data loss. The server does not have to reserve its resources for a single client for the indianite time that may pass between protocol messages. Another application for stateless protocols is information services that

divide the server load between several identical machines. The servers can be geographically distributed or clustered in one place. When the servers are stateless, client requests can be routed to an arbitrary server without giving any consideration to where the previous messages were processed. Routing decisions and reply addresses can be changed dynamically in order to level the load on the servers and to minimize communication costs.

Integrity and confidentiality of the state data:

When the state data is repeatedly transferred through insecure channels, its integrity and confidentiality become an important security concern. Since the state messages are sent and eventually received by the server itself, we can protect their integrity with message authentication codes that are relatively short and inexpensive to compute. Also, the freshness of the state data should be checked in order to limit the number of times the data can be replayed. Timestamps can be applied liberally, because they are checked by their creator against the same clock that is used for the time stamping. Expired messages can be simply ignored. (The client is responsible for taking any corrective steps after such error conditions.) It is, however, necessary to allow long lifetimes for the states so that the data does not expire before the client wants to continue the message exchange and succeeds in sending its next request. Hence, the timestamp lifetime should be longer than the expected duration of a denial-of-service attack, usually on the order of several hours or a few days. One consequence of time stamping is that distributed servers that accept state data packets created by each other must have synchronized clocks. Fortunately, the accuracy does not need to be very high if the timestamp lifetimes are long. The improved transformation of a tasteful service into a stateless one is illustrated by the protocol schema below. Every message leaving the server contains a time stamped state of the connection, authenticated with a key KsS known only by the server. The state is then returned to the server along the next message from the client.

Mitigation Methods:

Ad-hoc wireless sensor networks (WSNs) promise exciting new applications in the near future, such as ubiquitous on-demand computing power, continuous connectivity, and instantly-deployable communication for military and first responders. Such networks already monitor environmental conditions, factory performance, and troop deployment, to name a few applications. 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. Due to their ad-hoc organization, wireless ad-hoc networks are particularly vulnerable to denial of service (DoS) attacks [75], and a great deal of research has been done to enhance survivability [2, 5, 13, 14, 50, 75]. While these schemes can prevent attacks on the short-term availability of a network, they do not address attacks that affect long-term availability — the most permanent denial of service attack is to entirely deplete nodes' batteries. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper 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 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 [53, 59, 68], 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. Vampire attacks are not protocol-specific, in that they do not rely on design properties or implementation faults of particular routing protocols, but rather exploit general properties of protocol classes such as link-state, distance-vector, source routing, and geographic and beacon routing. Neither do these attacks rely on flooding the network with large amounts of data, but rather try to transmit as little data as possible to achieve the largest energy drain, preventing a rate limiting solution. Since Vampires use protocol-compliant messages, these attacks are very difficult to detect and prevent.

Protocols and Assumptions:

In this paper we consider the effect of Vampire attacks on link-state, distance-vector, source routing, and geographic and beacon routing protocols, as well as a logical ID-based sensor network routing protocol proposed by Parno et al. [53]. While this is by no means an exhaustive list of routing protocols which are vulnerable to Vampire attacks, we view the covered protocols as an important subset of the routing solution space, and stress that our attacks are likely to apply to other protocols. 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 re-discovery 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. Note that this is far from the strongest adversary model; rather this configuration represents the average expected damage from Vampire attacks. Intelligent adversary placement or dynamic node compromise would make attacks far more damaging. While for the rest of this paper we will assume 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. However, recall that sending any packet automatically constitutes amplification, allowing few Vampires to attack many honest nodes. We will show later that a single Vampire may attack every network node simultaneously, meaning that continuous recharging does not help unless Vampires are more resource-constrained than honest nodes. Dual-cycle networks (with mandatory sleep and awake periods) are equally

vulnerable to Vampires during active duty as long as the Vampire's cycle switching is in sync with other nodes. Vampire attacks may be weakened by using groups of nodes with staggered cycles: only active-duty nodes are vulnerable while the Vampire is active; nodes are safe while the Vampire sleeps. However, this defense is only effective when duty cycle groups outnumber Vampires, since it only takes one Vampire per group to carry out the attack.

Clean-Slate Sensor Network Routing:

The deployment of sensor networks in security- and safety-critical environments requires secure communication primitives. In this paper, we design, implement, and evaluate a new secure routing protocol for sensor networks. Our protocol requires no special hardware and provides message delivery even in an environment with active adversaries. We adopt a clean-slate approach and design a new sensor network routing protocol with security and efficiency as central design parameters. Our protocol is efficient yet highly resilient to active attacks. We demonstrate the performance of our algorithms with simulation results as well as an implementation on Telos sensor nodes.

The deployment of sensor networks in security- and safety-critical environments requires secure communication primitives. In this paper, we design, implement, and evaluate a new secure routing protocol for sensor networks. Our protocol requires no special hardware and provides message delivery even in an environment with active adversaries. We adopt a clean-slate approach and design a new sensor network routing protocol with security and efficiency as central design parameters. Our protocol is efficient yet highly resilient to active attacks. We demonstrate the performance of our algorithms with simulation results as well as an implementation on Telos sensor nodes.

References:

Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks, Eugene Y. Vasserman and Nicholas Hopper IEEE, and Yu-Chang Chao http://ieeexplore.ieee.org/xpl/articleDetails.jsp?arnumber=6175892

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.

M. Feldhofer, S. Dominikus, and J. Wolkerstorfer, "Strong Authentication for RFID Systems Using the AES Algorithm," Proc. Int'l Workshop Cryptographic Hardware and Embedded Systems(CHES), 2004.

R. Fonseca, S. Ratnasamy, J. Zhao, C.T. Ee, D. Culler, S. Shenker, and I. Stoica, "Beacon Vector Routing: Scalable Point-to-Point Routing in Wireless Sensornets," Proc. Second Conf. Symp.Networked Systems Design & Implementation (NSDI), 2005.

S. Galbraith, K. Harrison, and D. Soldera, "Implementing the Tate Pairing," Proc. Int'l Symp. Algorithmic Number Theory, 2002.

S. Goldberg, D. Xiao, E. Tromer, B. Barak, and J. Rexford, "PathQuality Monitoring in the Presence of Adversaries," Proc. ACM SIGMETRICS Int'l Conf. Measurement and Modeling of ComputerSystems, 2008.

X. Luo and R.K.C. Chang, "On a New Class of Pulsing Denial-of- Service Attacks and the

Defense," Proc. Network and Distributed System Security Symp. (NDSS), 2005.

M. Maleki, K. Dantu, and M. Pedram, "Power-Aware Sourc Routing Protocol for Mobile Ad Hoc Networks," Proc. Int'l Symp. Low Power Electronics and Design (ISLPED), 2002.

R. Govindan and A. Reddy, "An Analysis of Internet Inter- Domain Topology and Route Stability," Proc. IEEE INFOCOM, 1997.

M. Guirguis, A. Bestavros, I. Matta, and Y. Zhang, "Reduction of Quality (RoQ) Attacks on Internet End-Systems," Proc. IEEE INFOCOM, 2005.

J.L. Hill and D.E. Culler, "Mica: A Wireless Platform for Deeply Embedded Networks," IEEE Micro, vol. 22, no. 6, pp. 12-24, Nov./Dec. 2002.

Maidu, Johnson, and A. Lusin, "Ariadne: A Secure On- Demand Routing Protocol for Ad Hoc Networks," Proc. MobiCom, 2002.

Katiosantason "Packet Leashes: A Defense against Wormhole Attacks in Wireless Ad Hoc Networks," Proc.IEEE INFOCOM, 2003.

Nair.patal "Rushing Attacks and Defense in Wireless Ad Hoc Network Routing Protocols," Proc.Second ACM Workshop Wireless Security (WiSE), 2003.

Y. Huang and S. Bhatti, "Fast-Converging Distance Vector Routing for Wireless Mesh Networks," Proc. 28th Int'l Conf. Distributed Computing Systems Workshops (ICDCSW), 2008.

H. Eberle, A. Wander, N. Gura, C.-S. Sheueling, and V. Gupta,"Architectural Extensions for Elliptic Curve Cryptography over GF(2m) on 8-bit Microprocessors," Proc. IEEE Int'l Conf" Application Specific Systems, Architecture Processors (ASAP), 2005.

T. English, M. Keller, K.L. Man, E. Popovici, M. Schellekens, and .Marnane, "A Low-Power Pairing-Based Cryptographic Accelerator for Embedded Security Applications," Proc. IEEE Int'l SOC Conf. , 2009.

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.