A Trust-Aware Routing Framework for Wireless Sensor Networks to Avoid Vampire Attacks

[1]A. Selvi, [2]P. Elakkiya, [3]S. Gowsika
Department of Information Technology
M.Kumarasamy College of Engineering, Karur.
[1]Assistant Professor, [2,3]UG Scholar

***Abstract*— The multi-hop routing in wireless sensor networks (WSNs) offers little protection against identity deception through replaying routing information. The challenger can exploit this defect to launch various harmful or even devastating attacks against the routing protocols. This includes sink hole attacks, worm hole attacks and Sybil attacks. The situation is further provoked by mobile and harsh network conditions. The oldest cryptographic techniques or efforts at developing trust aware routing protocols do not effectively address this severe problem. To secure the Wireless sensor networks against adversaries misdirecting the multi-hop routing, the technique is designed and implemented using TARF, a robust trust aware routing framework for dynamic Wireless sensor networks. Without tight time synchronization or known geographic information, Trust aware routing framework provides trustworthy and efficient energy route.**

Keywords*— *Denial of service,Vampire attacks, security, routing, adhoc networks, sensor networks, wireless networks

I. INTRODUCTION

WIRELESS Ad hoc NETWORKS The main objective of an Ad-Hoc network is to maintain the node's connectivity and reliably transport the data packets. In addition, each node dynamically determines its next hop based on the network topology. WANET is one of the classifications of Ad-hoc networks.A wireless Ad-Hoc network,which is a decentralized network where each node (end-user node) is able to forward data packets for other nodes.The network is ad hoc because it does not rely on a pre existing infrastructure, such as routers in wired networks or access points in managed (infrastructure) wireless networks. Instead, each node participates in routing by forwarding data for other nodes, so the determination of which nodes forward data is made dynamically on the basis of network connectivity.

*A. Wireless Sensor Network*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, and a great deal of research has been done to enhance survivability. 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, 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.

B. Provably secure on demand source routing in mobile ad hoc networks

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 have 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 analyzed rigorously. 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 endair A, and we demonstrate the
usage of our framework by proving that it is secure in our model.

C. Protocols and assumptions

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. 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 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. 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 out number Vampires, since it only takes one Vampire per group to carry out the attack.

D. Security Threats

1) Vampire attack means the composition and transmission of a message that causes more energy to be consumed by the network than if an honest node transmitted a message of identical size to the same destination, although using different packet headers. We measure the strength of the attack by the ratio of network energy used in the benign case to the energy used in the malicious case, i.e., the ratio of network-wide power utilization with malicious nodes present to energy usage with only honest nodes when the number and size of packets sent remains constant. Safety from Vampire attacks implies that this ratio is 1.Energy use by malicious nodes is not considered, since they can always unilaterally drain their own batteries.
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

2)Denial-Of-Service Attacks The convenience of 802.11-based wireless access networks has led to widespread deployment in the consumer, industrial and military sectors. However, this use is predicated on an implicit assumption of confidentiality and availability. While the security flaws in 802.11's basic confidentially mechanisms have been widely publicized, the threats to network availability are far less widely appreciated. In fact, it has been suggested that 802.11 is highly susceptible to malicious denial-of-service (DoS) attacks targeting its management and media access protocols. This paper provides an experimental analysis of such 802.11-specific attack their practicality, their efficacy and potential low-overhead implementation changes to mitigate the underlying vulnerabilities

3)Defending against path based DoS attacks in wireless sensor networks 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 multi-hop 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*

F . Security Services

1)Data Verification – In data verification module, receiver verifies the path. Suppose data come with malicious node means placed in malicious packet. Otherwise data placed in honest packet. This way user verifies the data's.

2) Denial of service – In computing, a denial-of-service attack or distributed denial-of-service attack is an attempt

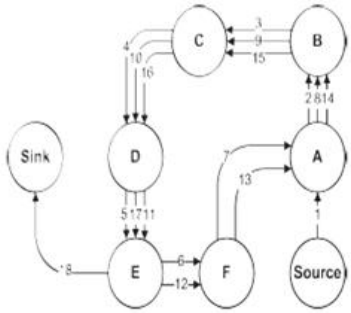
To make a meachine or a network resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of efforts to temporarily or indefinitely interrupt or suspend services of a host connected to the Internet.

3) User Module – In user module, verify user and any time create a new path. In security purpose user give the wrong details means display wrong node path otherwise display correct node path.

4) Stretch Attack – Stretch attack, where a malicious node constructs artificially long source routes, causing packets to traverse a larger than optimal number of nodes. An honest source would select the route Source → F → E → Sink, affecting four nodes including itself, but the malicious node selects a longer route, affecting all nodes in the network. These routes cause nodes that do not lie along the honest route to consume energy by forwarding packets they would not receive in honest scenarios.

II. PROBLEM DEFINITION

The first challenge in addressing Vampire attacks is defining them—what actions in fact constitute an attack? DoS attacks in wired networks are frequently characterized by amplification , an adversary can amplify the resources it spends on the attack, e.g., use 1 minute of its own CPU time to cause the victim to use 10 minutes. However, consider the process of routing a packet in any multihop network: a source composes and transmits it to the next hop toward the destination, which transmits it further, until the destination is reached, consuming resources not only at the source node but also at every node the message moves through. If we consider the cumulative energy of an entire network, amplification attacks are always possible, given that an adversary can compose and send messages which are processed by each node along the message path. So, the act of sending a message is in itself an act of amplification, leading to resource exhaustion, as long as the aggregate cost of routing a message (at the intermediate nodes) is lower than the cost to the source to compose and transmit it. So, we must drop amplification as our definition of maliciousness and instead focus on the cumulative energy consumption increase that a malicious node can cause while sending the same number of messages as an honest node. In the attack, an adversary composes packets with purposely introduced routing loops. We call it the carousel attack (in Existing Method), since it sends packets in circles as shown in 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.



III. LITERATURE REVIEW

R.Prema, R.Rangarajan [1] This paper deals with Several wireless sensor network applications ought to decide the intrinsic variance between energy efficient communication and the requirement to attain preferred quality of service (QoS) such as packet delivery ratio, delay and to reduce the power consumption of wireless sensor nodes. In order to address this challenge, we propose the Power Aware Routing Protocol (PARP), which attains application-specified communication delays at low energy cost by dynamically adapting transmission power and routing decisions. Extensive simulation results prove that the proposed PARP attains better QoS and reduced power consumption. This paper proposed power aware routing protocol for wireless sensor network. Power Aware Routing Protocol uses link quality estimation and power aware routing which results in reduced power consumption and delay with increased packet delivery ratio. David R. Surma, Edwin H-M. Sha, Nelson Passos [2] proposed a Communication Scheduling with Re-routing based on Static and Hybrid Techniques In massively parallel systems, the performance gains are often significantly diminished by the inherent communication overhead. This overhead is caused by the required message passing resulting from the task allocation scheme. In this paper, techniques to reduce this communication overhead by both scheduling the communication and determining the routing that the messages should take within a tightly coupled processor network are presented. Using the recently developed Collision Graph model, static scheduling algorithms are derived which work at compile time to determine the ordering and routing of the individual message transmissions. Since a priori knowledge about the network track required by static scheduling may not be available or accurate, this work also considers dynamic scheduling. A novel hybrid technique is presented which operates in a dynamic environment yet uses known information obtained by analyzing the communication patterns. Experiments performed show significant improvement over baseline techniques. While working on massively parallel systems, it was found that the communication over head greatly impacted the system performance. To reduce this overhead, techniques were derived to perform scheduling at a very low level by considering individual message transfers. In a static

environment, the SCORE algorithm was developed and shown to provide improvement of over 20% as compared to a baseline approach. This algorithm uses the newly developed Collision Graph to determine both a schedule and the routing scheme for the message transmissions. Since the information required by static techniques is not always readily available or accurate, the HYCORE technique was developed to operate but with knowledge obtained by a compile-time analysis. Again, improvements of approximately 20% were obtained. Together, the Collision Graph and this scheduling strategy form a framework for which continued study into communication scheduling can be done. Gergely A.cs, Levente Buttya.n, and Istva.n Vajda [3] 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 have mainly been analyzed by informal means only. This paper, deals that flaws in ad hoc routing protocols can be very subtle, and we advocate a more systematic way of analysis and proposes a mathematical framework in which security can be precisely defined, and routing protocols for mobile ad hoc networks can be analyzed rigorously. The framework is tailored for on demand source routing protocols, but the general principles are applicable to other types of protocols too and the approach is based on the simulation paradigm, which has already been used extensively for the analysis of key establishment protocols, but to the best, it has not been applied in the context of ad hoc routing so far. This paper also propose a new on-demand source routing protocol, called endairA, and demonstrated the usage of the framework by proving that it is secure model.The main message of this paper is that attacks against ad hoc routing protocols can be subtle and difficult to discover by informal reasoning about the properties of the protocol.

Zhijun Li, Guang Gong [4] Wireless sensor networks are vulnerable to the node clone, and several distributed protocols have been proposed to detect the attack. However, they require too strong assumptions to be practical for large-scale, randomly deployed sensor networks. Sensor nodes lack tamper-resistant hardware and are subject to the node clone attack. This paper, proposes two novel node clone detection protocols with different trade offs on network conditions and performance. The first one is based on a distributed hash table (DHT), by which a fully decentralized, key-based caching and checking system is constructed to catch cloned nodes effectively.The protocol performance on efficient storage consumption and high security level is theoretically deducted through a probability model, two distributed detection protocols: One is based on a distributed hash table, which forms a Chord overlay network and provides the key-based routing, caching, and checking facilities for clone detection, and the other uses probabilistic directed technique to achieve efficient communication overhead for satisfactory detection .Although the DHT-based protocol incurs similar communication cost as previous approaches, it may be considered a little high for some scenarios and it provides high security level for all kinds of sensor networks by one deterministic witness and additional memory-efficient, probabilistic witnesses, the randomly directed exploration presents outstanding communication performance and minimal storage consumption for dense sensor networks. To address this concern, the second distributed detection protocol, named randomly directed exploration, presents good communication performance for dense sensor networks, by a probabilistic directed forwarding technique along with random initial direction and border determination. The simulation results uphold the protocol design and show its efficiency on communication overhead and satisfactory detection.

IV. PROPOSED SOLUTION

In proposed system we are going to show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network method to provably bound the damage from Vampire attacks during packet forwarding.In our proposed system we are going to implement SEAD protocol using Bellman Ford Algorithm which is more secure.

1) SEAD : Secure Efficient Ad-Hoc Distance Protocol

An ad hoc network is a collection of wireless computers (nodes), communicating among themselves over possibly multihop paths, without the help of any infrastructure such as base stations or access points. Although many previous ad hoc network routing protocols have been based in part on distance vector approaches, they have generally assumed a trusted environment. In this paper, we design and evaluate the Secure Efficient Ad hoc Distance vector routing protocol (SEAD), a secure ad hoc network routing protocol based on the design of the Destination-Sequenced Distance-Vector routing protocol. In order to support use with nodes of limited CPU processing capability, and to guard against Denialof- Service attacks in which an attacker attempts to cause other nodes to consume excess network bandwidth or processing time, we use efficient one-way hash functions and do not use asymmetric cryptographic operations in the protocol. SEAD performs well over the range of scenarios we tested, and is robust against multiple uncoordinated attackers creating incorrect routing state in any other node, even in spite of any active attackers or compromised nodes in the network.

This Project makes three primary contributions.

1)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 secure routing protocols such as Ariadne, SAODV, and SEAD do protect against Vampire attacks. The 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.

2)Second, we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary).
3)Third, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

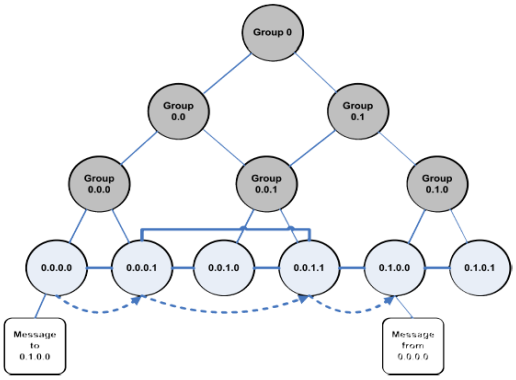


Figure 5.1 Secure Architecture using SEAD Protocol

The final address tree for a fully-converged 6-node network. Leaves represent physical nodes, connected with solid lines if within radio range. The dashed line is the progress of a message through the network. Note that non-leaf nodes are not physical nodes but rather logical group identifiers.

Bellman-Ford Algorithm

This algorithm iterates on the number of edges in a path to obtain the shortest path. Since the number of hops possible is limited (cycles are implicitly not allowed), the algorithm terminates giving the shortest path.

V. REFERENCES

[1] Eugene Y. Vasserman and Nicholas Hopper "Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks"- IEEE transactions on mobile computing, vol. 12, no. 2, February 2013.
[2] David R. Surma , Edwin H-M. Sha , Nelson Passos "Communication Scheduling with Re-routing based on Static and Hybrid Techniques" June 2013.
[3]Gergely A.cs, Levente Buttya.n, and Istva.n Vajda "Provably Secure On-demand Source Routing in Mobile Ad Hoc Networks" March 2005.
[4] Kunal Vikas Patil, M.R.Dhage "The Adaptive Optimized Routing Protocol for Vehicular Ad-hoc Networks" June 2013.
[5] Packet leashes " A defence against wormhole attacks in wireless ad hoc networks" infocom, 2003.