www.ijiarec.com

ISSN:2348-2079

Volume-5 Issue-2

International Journal of Intellectual Advancements and Research in Engineering Computations

Defending against energy draining attacks in wireless sensor networks with secure synchronization

1.Mr.S.Jagadeesan,M.Sc.,M.C.A.,M.Phil.,M.E., Assistant Professor
2. Mr. T.Vinoth, Final M.C.A.
Department of MCA, Nandha Engineering College,(Autonomous), Erode-52.
jagadeesan12398@gmail.com, vinoththangaveln@gmail.com

Abstract— Wireless ad-hoc sensor network are promise exciting new application and deployable and security communication for networking. Ad hoc wireless network is fixed frequency communication between sensor nodes, so low power consumption and high security provide in ad hoc network. Vampire attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. It is found 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. Carousel attack and Stretch attack are the possible scenarios occurred. To avoid such attacks attestation based forwarding scheme and loose source routing is proposed. In addition thesis, avoid carousel attack and stretch attack consider to multiple system, because attestation based forwarding and loose source routing process travel the packet one to many shortest path from the multiple node, so address energy efficiency problem the algorithms propose by synchronizing the transmission times of all the nodes in the system. The thesis proposes the concepts using Content and Presence Multicast Protocol (CPMP) using the FPD (Future Peak Detection) and RFPD (Randomized Future Peak Detection) algorithms which nodes use to send updates to their neighbors. The updates contain the relative time of their sender's next transmission.

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

INTRODUCTION

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. This is an instance of a resource depletion attack, with battery power as the resource of interest. In this paper, they consider how routing protocols, even those designed to be secure, lack protection from these attacks, which they 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. 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.

DENIAL OF SERVICE RESILIENCE IN AD HOC NETWORKS

Significant progress has been made towards making ad hoc networks secure and DoS resilient. However, little attention has been focused on quantifying DoS resilience: In this paper [1], they design and study DoS attacks in order to assess the damage that difficult- to-detect attackers can cause. The first attack, called the JellyFish attack, is targeted against closed-loop flows such as TCP; although protocol compliant, it has devastating effects. The second is the Black Hole attack, which has effects similar to the JellyFish, but on open-loop flows. They quantify via simulations and analytical modeling the scalability of DoS attacks as a function of key performance parameters such as mobility, system size, node density, and counter-DoS strategy. One perhaps surprising result is that such DoS attacks can increase the capacity of ad hoc networks, as they starve multi-hop flows and only allow one-hop communication, a capacity-maximizing, yet clearly undesirable situation.

The goal of this paper is to quantify via analytical models and simulation experiments the damage that a successful attacker can have on the performance of an ad hoc network. In particular, they recognize that successful attacks are inevitable (at least until the corresponding counter-DoS protocol modification is deployed), and our objective is to characterize the relationship between the resources that must be commandeered by the attacker (the percentage of nodes in an ad hoc network used in the attack) and the impact on performance of non-attacking nodes, where performance refers to per-flow good put and system-wide fairness. In this way, they study the scalability of DoS attacks and identify the key mechanisms and factors of both attacks and protocols that affect a system's DoS resilience.

The goal of JF nodes is to reduce the good put of all traversing flows to near-zero while dropping zero or a small fraction of packets. In particular, JF nodes employ one of three mechanisms. The first JF variant is a packet misordering attack. TCP has a well- known vulnerability to misordered packets due to factors such as route changes or the use of multi-path routing, and a number of TCP modifications have been proposed to improve robustness to misordering [12]. However, no TCP variant is robust to malicious and persistent reordering as employed by the JF misordering attack.

In particular, suppose that congestion losses force a node to drop x% of packets. As shown , if these losses occur periodically at the retransmission-time-out timescale (approximately 1 second), TCP throughput is reduced to near zero even for small values of x. Thus, a JF periodic-dropping node can drop no more packets than neighboring congested nodes, but inflict near-zero throughputs on all TCP flows traversing it.

Finally, in addition to the JF attack, they also study the "black hole" attack as described . This attack is relevant for open- loop flows that do not respond to congestion, loss, or delay information, and hence cannot be thwarted by JellyFish. Black Hole nodes participate in the routing protocol to establish routes through themselves, yet drop all packets after correctly receiving them at the MAC layer. With these attacks (three JF variants and Black Holes), they use a combination of analytical modeling and simulation experiments to study the key performance factors that determine a network's DoS resilience and equivalently, the attack's scalability.

Finally, they study a number of system factors that affect a network's DoS resilience and obtain the following findings. (i) JF have a network partitioning effect that severely degrades or altogether prevents long-range communication. Consequently, an increased number of JF reduce the system's fairness index but increase network capacity, as capacity can be increased by starving long-range flows and serving only one-hop flows. (ii) The mean and distribution of path length have a significant effect on attack scalability as higher path length flows are highly vulnerable. (iii) JF is most devastating in a system with a well balanced offered load.

Thus, our goal is not to advance the aforementioned "arms race" by developing attacks, victim counter strategies, counter attacks, etc., but rather to explore the impact of a class of attacks that are difficult and time consuming to detect due to their compliance to all protocol rules.

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 has been analyzed either by informal means only, or with formal methods that have never been intended for the analysis of this kind of protocols. In this paper, they present a new attack on Ariadne, a previously published “secure” routing protocol . Other attacks can be found.

Routing has two main functions: route discovery and packet forwarding. The former is concerned with discovering routes between nodes, whereas the latter is about sending data packets through the previously discovered routes. There are different types of ad hoc routing protocols. One can distinguish proactive (e.g., OLSR) and reactive (e.g., AODV and DSR) protocols. Protocols of the latter category are also called on-demand protocols.

In this paper [2], they focus on the route discovery part of on-demand source routing protocols, but they believe that the general principles of our approach are applicable to the route discovery part of other types of protocols too. At a very informal level, security of a routing protocol means that it can perform its functions even in the presence of an adversary

Regarding the capabilities of the adversary, they assume that it can mount active attacks (i.e., it can eavesdrop, modify, delete, insert, and replay messages) from corrupted nodes that have the same communication capabilities as the nodes of the honest participants in the network. This means that the adversary is not all powerful, and it cannot fully control the communication of the honest participants; it can receive only those messages that were transmitted by one of its neighbors, and its transmissions can be heard only by its neighbors.

The mathematical framework that they introduce in this paper is based on the so called simulation paradigm. This has been successfully used in the analysis of some cryptographic algorithms and some cryptographic protocols. However, it has never been applied in the context of ad hoc routing protocols. One of the main contributions of this work is the application of this approach in a new context.

A preliminary result of this work has been presented. However, in that paper, they considered only an Active-1-1 adversary, and they did not allow parallel protocol runs. In this paper, they extend their previous results to an Active-y -x adversary, where x; y ¸ 1, and they allow the simultaneous execution of any number of instances of the route discovery protocol.

INSENS: INTRUSION-TOLERANT ROUTING IN WIRELESS SENSOR NETWORKS

This paper [5] describes an Intrusion-tolerant routing protocol for wireless Sensor NetworkS (INSENS). INSENS constructs forwarding tables at each node to facilitate communication between sensor nodes and a base station. It minimizes computation, communication, storage, and bandwidth requirements at the sensor nodes at the expense of increased computation, communication, storage, and bandwidth requirements at the base station. INSENS does not rely on detecting intrusions, but rather tolerates intrusions by bypassing the malicious nodes.

Wireless sensor networks (WSNs) are rapidly emerging as an important new area in mobile computing research. Applications of WSNs are numerous and growing, and range from indoor deployment scenarios in the home and office to outdoor deployment scenarios in natural, military and embedded environments.

In each of these scenarios, lives and livelihoods may depend on the timeliness and correctness of the sensor data obtained from dispersed sensor nodes. As a result, such WSNs must be secured to prevent an intruder from obstructing the delivery of correct sensor data and from forging sensor data.

The design and implementation of secure WSNs must simultaneously address several difficult research challenges. First, wireless communication among the sensor nodes increases the vulnerability of the network to eavesdropping, unauthorized access, spoofing, replay and denial-of-service (DOS) attacks. Second, the sensor nodes themselves are highly resource-constrained in terms of limited memory, CPU, communication bandwidth, and especially battery life.

To achieve intrusion tolerance given an asymmetric topology and resource constraints, this paper presents an intrusion-tolerant routing protocol for wireless sensor Networks (INSENS). The INSENS secure routing system adheres to the following high-level design principles. First, to prevent DOS-style flooding attacks, the type of communication is constrained. Individual nodes are not allowed to broadcast to the entire network. Only the base station is allowed to broadcast.

They describe later on how authentication of the base station is achieved via one-way hashes, so that individual nodes cannot spoof the base station and thereby flood the network. For unicast packets, nodes must first communicate through the base station, allowing the base station to act as a packet filter to prevent DOS via a single node.

Third, to address resource constraints, INSENS follows two design decisions: symmetric key cryptography is chosen for confidentiality and authentication between the base station and each resource-constrained sensor nodes, since it is considerably less compute-intensive than public key cryptography; and, the base station is chosen as the central point for computation and dissemination of the routing tables. Fourth, to address the notion of compromised nodes, redundant multi path routing is built into INSENS to achieve secure routing.

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 [6] 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.

They 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. They 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.

Ad hoc routing protocols can be broadly classified as table driven routing protocols and source initiated on- demand routing protocols . The first approach uses a routing table which is maintained via periodic updates from all the other nodes in the network irrespective of the fact that the network may not be active in terms of data traffic.

Prior studies have been aimed at designing minimum energy routing protocols. Subbarao suggests a minimum power routing scheme that has been designed using the table-driven approach. Singh et al. introduce power aware cost metrics for routes and design routing schemes that minimize these metrics.

A distributed position based network protocol that uses location information to compute a multi-hop route which minimizes the energy to deliver the packet. Chang et al. [30] propose algorithms to select routes and corresponding power levels in a static wireless ad hoc network such that the system lifetime (in terms of battery life) is maximized. Xu et al.

Energy savings are achieved by keeping certain chosen coordinator nodes active while the other nodes in the network are in a power save mode. The design of physical layer aware s protocols, algorithms and applications are minimize energy consumption of the system and individual nodes. The effect of the entire hardware architecture on the design of protocols and algorithms is considered. Brown et al. [34] study the fairness of different power aware routing objectives.

Their experimental results justify the necessity of the required features of a minimum energy routing protocol. These features are very generic in nature and can be used as a guideline for designing new minimum energy routing protocols. They have shown that these features can be easily implemented on an existing version of the protocol to derive a ’minimum energy routing’ version of the protocol.

RELIABLE BROADCAST IN UNKNOWN FIXED-IDENTITY NETWORKS

In this paper, we formulate a new theoretical problem, namely the reliable broadcast problem in unknown fixed identity networks . This problem arises in the context of developing decentralized security mechanisms in a specific class of distributed systems: Consider an undirected graph G connecting n nodes where each node is aware of only its neighbors but not of the entire graph. Additionally, each node has a unique identity and cannot fake its identity to its neighbors. Assume that k among the n nodes act in an adversarial manner and the remaining n − k are good nodes.

Reliable communication between nodes in the presence of byzantine dversaries is a fundamental problem in distributed a system that was first considered in the context of the classic Byzantine General's problem. Consider a network G = (V,E) where the edges in E represent reliable channels between nodes in V.

The sparse network results have important ramifications for Internet routing. The Internet topology at the autonomous system is 1 − connected and therefore cannot handle even a single adversarial node.

ARCHITECTURAL EXTENSIONS FOR ELLIPTIC CURVE CRYPTOGRAPHY OVER GF (2M)

In this paper, they examine hardware extensions at the micro architecture level to accelerate public-key operations with elliptic curve cryptography (ECC). While the extensions proposed are generic in that they can be applied to any general purpose processor, this paper addresses their implementation on 8-bit microprocessors**.**

Typically, acceleration of public-key cryptosystems is achieved through dedicated coprocessors. Here, they want to explore an alternative approach that provides hardware acceleration through extensions of an existing data path of a general-purpose processor.

Due to its computational effect, ECC is emerging as an attractive alternative to traditional public-key cryptosystems such as RSA, DSA, and DH. More specially, ECC offers equivalent security with smaller key sizes, resulting in reduced computation time and lower memory requirements.

Elliptic curves have been standardized by NIST and SECG for fields GF (p) and GF (2m). Though both types of fields offer similar security strengths, the standards offer a choice to accommodate different implementation platforms. While arithmetic operations over fields GF (p) directly map to integer operations found in standard processors, operations over fields GF (2m) are supported rather inefficiently.

On the 8-bit ATmega128 microprocessor running at 8 MHz they measured an execution time for a 163-bit ECC point multiplication over GF (2m) of 0.4 s with the extended multiplier and 0.29 s if, in addition, a multiply-accumulate instruction is provided. In comparison, a 1024-bit RSA private-key operation providing equivalent security strength takes 11s.

Arithmetic in GF (2m) briefly introduce the arithmetic operations needed to implement ECC point multiplication over binary polynomial fields GF (2m)[1]. The operations include modular addition, subtraction, multiplication, squaring, and division, where the operands are polynomials with coefficients of either 0 or 1.

AN ENERGY CONSUMPTION MODEL FOR PERFORMANCE ANALYSIS OF ROUTING PROTOCOLS

A mobile ad hoc network (or MANEt) is a group of mobile, wireless nodes which cooperatively form a network independent of any fixed infrastructure or centralized administration. In particular, a MANET has no base stations: a node communicates directly with nodes within wireless range and indirectly with all other nodes using a dynamically-computed, multi-hop route via the other nodes of the MANET.

Simulation and experimental results are combined to show that energy and bandwidth are substantively different metrics and that resource utilization in MANEt routing protocols is not fully addressed by bandwidth-centric analysis.

Energy consumption at the network interface is an issue for all mobile computing devices, whether they operate within a base station infrastructure or in a free-standing mobile ad hoc network (manet). Though universally recognized as an important issue in the design of manet protocols, energy consumption has not been used as a criteria in their evaluation.

Two well-studied protocols, Dynamic Source Routing (DSR) and Ad hoc On-demand Distance Vector (AODV) were examined using this strategy. The results validate the hypothesis: energy consumption and bandwidth utilization are substantively different metrics because the former takes into account the costs of both sending and receiving traffic and emphasizes the differences between broadcast and point-to-point communication. More specific observations include:

The “broadcast flooding” process used in route discovery is expensive for both DSR and AODV, but particularly for the latter.

For DSR, source routing headers are a noticeable, but not dominating cost. Operating the network interface in promiscuous mode is a significant cost.

Link-layer costs associated with the ad hoc environment are potentially extremely significant.

In Mobile ad hoc networks Wireless Local or Metropolitan Area networks consist of a group of mobile nodes and a much smaller number of base stations or access points. The mobile nodes are usually small, battery-powered elements. The base stations are at fixed locations and have an unlimited energy store.

By contrast, a MANET is a wireless network that operates independently of any fixed infrastructure or central administration. A node communicates directly with nodes within wireless range and indirectly with other nodes using dynamically computed routes through the nodes of MANET. In effect, all nodes are routers, participating in some protocol by which routes are discovered and maintained. A MANET is characterized by energy-constrained mobile nodes, bandwidth- constrained, variable-capacity links and unpredictable, dynamic topology.

The high-level contribution of this work is confirmation of the hypothesis that resource utilization in ad hoc routing protocols is not fully addressed by evaluations which consider only bandwidth. Protocol performance analyses which do not take energy consumption into account may overlook problems that would hinder its practical use. Regardless of whether a protocol developer chooses to apply a particular energy consumption calculation, performance analyses must consider node density, the proportion of broadcast and point- to-point traffic, message size and promiscuous mode operation at the network interface.

More specifically, this work defines a energy consumption model that is both suitable for use with traffic and mobility-oriented simulation of mobile ad hoc networks and based on experimental characterization of a common wire- less network interface. high and nodes are exposed to all traffic within wireless range.

The energy consumption of receiving and discarding traffic is both substantial and disproportional to the number of packets or bytes transmitted.

Because the cost of discarding traffic is low relative to the idle mode power consumption, the cost of operating the interface in promiscuous mode is high.

Broadcasting is expensive, especially if the node density is high. “Broadcast flooding” is a very expensive operation.

The incremental costs associated with a packet are relatively small compared to the fixed costs. The number of packets has greater impact on energy consumption than packet size does.

DSR is the most efficient of the three protocols in terms of packets sent and received. At high mobility, it is also the most efficient in terms of the number of bytes. However, this bandwidth efficiency is obtained at the cost of energy efficiency. Because nodes running DSR eaves drop on the source routing headers of all the traffic being forwarded by nodes in their one-hop neighborhood, their route caches can reflect a large fraction of the network topology.

2.8 BEACON VECTOR ROUTING: SCALABLE POINT-TO-POINT ROUTING IN WIRELESS SENSORNETS

The first generation of sensor net deployments focused primarily on data collection. In support of this task, most current sensor net code bases offer only the basic tree-based many-to-one and one-to-many routing primitives; protocols such as Directed Diffusion, TAG and others build trees that can both broadcast commands and collect data, with various forms of aggregation along the collection path.

Unfortunately, it is hard to test these ideas because there is currently no practical and broadly-applicable implementation of point-to-point routing for sensor nets. We know of two implementations of a reduced AODV and of GPSR, but they haven't been reported on in the literature. As we discuss in the next section, they have limitations on their applicability. It isn't clear how important these newly proposed uses are, but without a point-to-point routing protocol we will never be able to evaluate their true utility.

Geographic Coordinates: A different and potentially attractive solution for sensor networks is based on geographic routing. Here, nodes are identified by their geographic coordinates and routing is done greedily; at each step, nodes pick as next-hop the neighbor that is closest to the destination. When a node has no neighbor that is closer to the destination, these protocols enter perimeter mode, where the right-hand rule is used to forward a packet along a planarized subgraph until it reaches a node closer to the destination than the starting point of perimeter mode (then it resumes its greedy forwarding).

Second, and more seriously, such routing requires that each node know its geographic coordinates. While there are some sensor nodes that are equipped with GPS, the most widely used node, the Berkeley mote, is not. Moreover, even when available, GPS does not work in certain physical environments and the various proposed localization algorithms are not precise enough (at least not in all settings) to be used for geographic routing. Finally, even ignoring all the above, greedy geographic may be substantially suboptimal because it does not use real connectivity information and geography.

EXISTING SYSTEM

In existing system, two attacks are considered and solved. These are carousel attack and stretch attack. Since the stretch attack is more challenging to prevent, its success rests on the forwarding node not checking for optimality of the route. If we call the no-optimization case “strict” source routing, since the route is followed exactly as specified in the header, loose source routing is defined, 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. For carousel attack prevention, independent checking of packet progress is considered: if nodes keep track of route “cost” or metric and, when forwarding a packet, communicate the local cost to the next hop, that next hop can verify that the remaining route cost is lower than before, and therefore the packet is making progress toward its destination.

DRAWBACKS OF EXISTING SYSTEM

The existing system has following disadvantages,

- Only attack scenario is treated. Detaching malicious node from the network is not considered.
- The suspicious node cannot be tracked in inflation attack scenario.
- The path can be stretched by intermediate nodes, if packet modification privilege is given to them.
- A fully satisfactory solution for Vampire attacks during the topology discovery phase is not offered.

PROPOSED SYSTEM

The proposed system includes all the existing system implementation. In addition, secure synchronization is carried out. The new system eliminates the synchronization problem by calculating the transmission schedule using the weight information based on the proposed algorithm steps. In addition, synchronizing all the neighbor nodes which belong to various clusters, must to attain the stable state of the network.

The proposed system present techniques for synchronizing nodes that periodically broadcast content and presence updates to collocated nodes over an ad hoc network. Instead of aligning duty cycles, the new algorithms synchronize the periodic transmissions of nodes. This allows nodes to save battery power by switching off their network cards without missing updates from their neighbors. The proposed system is able to disrupt synchronization even when launched by a single attacker.

Advantages of the Proposed System

The advantages are listed below:

- In addition to Vampire attack, Inflation attack scenario is also prevented.
- Weight based synchronization if works with correct weight information chooses the correct cluster for the given node.
- Future peak detection scenario makes the correct cluster identification and avoids the inflation attack induced by the malicious nodes which sends wrong weight information.
- The suspicious node can be tracked easily since it does not satisfy the node behaviors of neighbor nodes.

CONCLUSION

The central question addressed is how to effectively exploit secondary user co-operation when conventional cooperation method becomes inefficient. FLEC, a flexible channel cooperation design is proposed to allow SUs to customize the use of leased resources in order to maximize performance. The problem of synchronizing the periodic transmissions of nodes in ad hoc networks, in order to enable battery lifetime extensions without missing neighbor's updates is studied. Several solutions, both lightweight and scalable but vulnerable to attacks is proposed.

Extension of generic algorithm to use transmission stability as a metric for synchronization is made. The implementation and simulations show that the protocols are computationally inexpensive, provide significant battery savings, are scalable and efficiently defend against attacks.

REFERENCES

[1] "The Network Simulator - ns-2," http://www.isi.edu/nsnam/ns 2012.

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

[3] G. Acs, L. Buttyan, and I. Vajda, "Provably Secure On-DemandSource Routing in Mobile Ad Hoc Networks," IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

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

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