Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 3, Issue. 2, February 2014, pg.716 – 720

RESEARCH ARTICLE

Vampire Attacks: Topology Discovery in Wireless Ad Hoc Sensor Networks

P. Dhivya[1], P. Sathya Priya[2], M. Thenila[3]

[1]Computer Science & Engineering Department & Anna University, India
[2]Computer Science & Engineering Department & Anna University, India
[3]Computer Science & Engineering Department & Anna University, India
[1] divi15.p@gmail.com; [2] sathyapr03@gmail.com; [3] thenilakumar@gmail.com

Abstract— This Project work explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining nodes battery power. The "Vampire" attacks are not specific to any specific protocol, but rather rely on the properties of many popular classes of routing protocols. To mitigate these types of attacks, include a new proof-of-concept protocol and AODV protocol that provably bounds the damage caused by Vampires during the packet forwarding phase.

Keywords—Ad-Hoc network; Stretch attack; Carousel attack; Vampire attack; Sensor network

I. INTRODUCTION

Ad Hoc wireless sensor network 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 project, it consider how routing protocols, even those designed to be secure, lack protection from these attacks, which 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. 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.

This project makes three primary contributions: First, we thoroughly evaluate the vulnerabilities of existing protocols to routing layer battery depletion attacks. This project 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, and SEAD 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 behaviour and cannot optimize out malicious action.

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

II. LITERATURE SURVEY

A. A Clean Slate Approach

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

Sensor Networks provide economically viable solutions for a wide variety of applications, including surveillance of critical infrastructure, safety monitoring, and many health care applications. As sensor networks are increasingly deployed in such security- and safety critical environments, the need for secure communication primitives is self-evident. Likewise, the development of secure primitives enables the use of sensor networks in new applications. The central goal of this work is to ensure node-to-node message delivery, even if the sensor network is under active attack. In the presence of an attacker, it is an extremely challenging task to maintain correct routing information, the attacker could inject malicious routing information or alter legitimate routing setup or update messages. Even, when route setup or update messages are authenticated, compromised sensor nodes can supply incorrect routing information of their own and cripple the routing infrastructure. Most proposals for sensor network routing protocols assume a trusted environment and cannot function under attacks two exceptions are INSENS, which routes only between nodes and a central base station, and SIGF, which relies on nodes knowing their geographic location.

B. Secure Neighbour Discovery in Wireless Networks

Wireless communication enables a broad spectrum of applications, ranging from commodity to tactical systems. Neighbor discovery (ND), that is, determining which devices are within direct radio communication, is a building block of network protocols and applications, and its vulnerability can severely compromise their functionalities. A number of proposals to secure ND have been published, but none have analysed the problem formally. In this project, it contributes such an analysis: build a formal model capturing salient characteristics of wireless systems, most notably obstacles and interference, and it provide a specification of a basic variant of the ND problem. Then, this project derives an impossibility result for a general class of protocols it term time-based protocols to which many of the schemes in the literature belong. This project also identifies the conditions under which the impossibility result is lifted. Moreover, this project explores a second class of protocols it term time and location-based protocols and prove they can secure ND.

Wireless networking is a key enabler for mobile communication systems that range from cellular infrastructure-based data networks and wireless local area networks (WLANs) to disaster-relief, tactical, and sensor networks, and short range wire replacement and radio frequency identification (RFID) technologies. In all such systems, any two wireless devices communicate directly when in range, without the assistance of other devices. The ability to determine if direct, one-hop, communication takes place is fundamental. For example, a WLAN access point (AP) assigns a new IP address to a mobile station only when it is within the APs coverage area. Or, a mobile node does not initiate a route discovery across a mobile ad hoc network (MANET) if a sought destination is already in its neighbor table. Or, an RFID tag will be read only if the signal transmitted by the tag can be received directly by the reader. These examples illustrate that, depending on whether another system entity, denoted as node in the rest of the paper, is a neighbor or not, actions are taken (e.g., by the AP or the router) or implications are derived (e.g., the RFID tag and reader are physically close). In other words, discovering a neighbor, or knowing that a node is a neighbor, is a common building block and enabler of diverse system functionality.

Nonetheless, if an attack against neighbor discovery (ND) can be perpetrated, such functionality can be abused. For example, letting legitimate nodes erroneously believe that they are neighbors allows the adversary to fully control communication across these artificial links. The threat lies in that the attacker can deny or derange communication at any point; this can happen exactly at the moment a message critical for the system operation is transmitted. In multi-hop networks, a well chosen artificial link is likely to attract a considerable number of routes, with devastating effects such as denial of communication across all these routes and significant disturbance of data. In a different scenario, misleading an RFID tag reader that the tag (and its owner) is physically close to the RFID reader, while this is not so, can enable the adversary to gain unauthorized access to the premises of the tag owner.

III. **MODULES SPLIT UP**

A. Sensor Node Creation

In this module, it creates many sensor nodes. This evaluates both the carousel and stretch attacks in a randomly generate a node topology. The source node sends the packets through nodes using protocols. Source node checks the path using routing protocols. It can capable of performing some processing, gathering sensor information and communicating with other connected nodes in the network.

B. Sensor Node Activation

In this module, it creates to activate the sensor nodes. Sensor node will used to sense the data. Sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding. Wireless sensor networks are also used for the collection of data for monitoring of environmental information.

C. Monitoring Sensor Information

Ad hoc wireless networks has primarily dealt with adversaries who prevent route setup, disrupt communication, or preferentially establish routes through themselves to drop, manipulate, or monitor packets. Nodes send messages to aggregators, in turn sends it to other aggregators, which route it to a monitoring point. However, nearby nodes might be able to monitor communication to detect link failure.

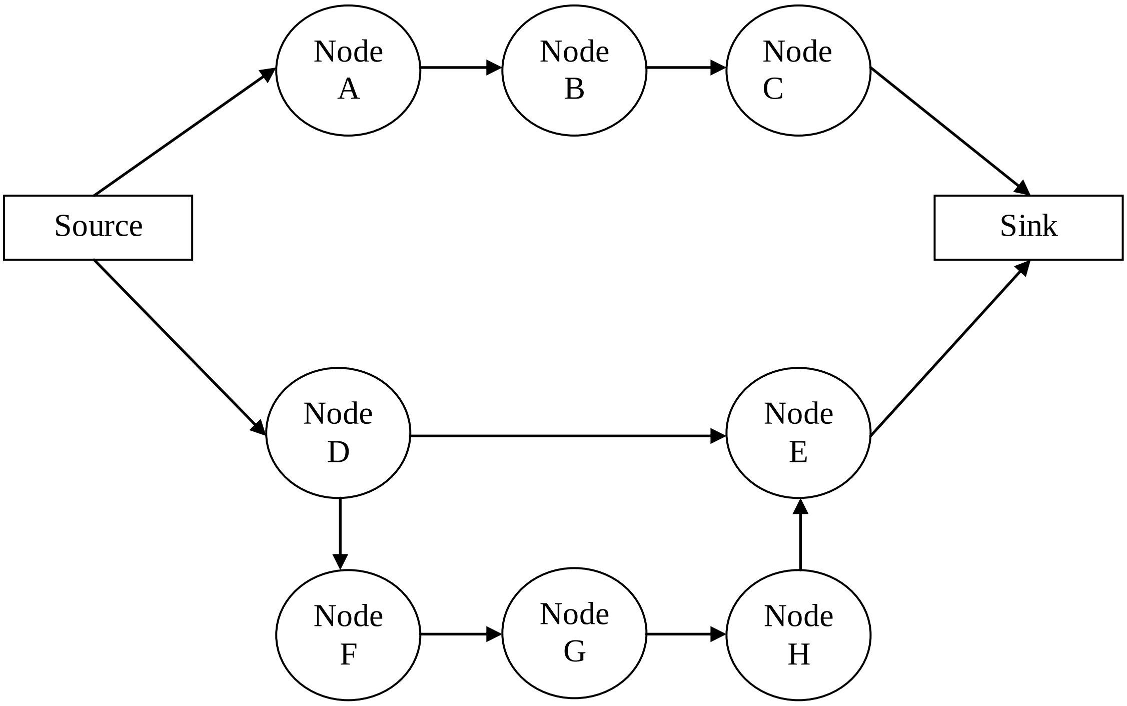

Fig. 1 Monitoring Sensor Information

D. Types of Attacks

In **Carousel attack**, an adversary sends a packet with a route composed as a series of loops, such that the same node appears in the route many times. This strategy can be used to increase the route length beyond the number of nodes in the network, only limited by the number of allowed entries in the source route.

In **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 -> sink, affecting nodes including it, but the malicious node selects a longer route, affecting all nodes in the network.

E. Attacks on Stateless Protocols

In these systems, the source node specifies the entire route to a destination within the packet header, so intermediaries do not make independent forwarding decisions, relying rather on a route specified by the source. To forward a message, the intermediate node finds itself in the route (specified in the packet header) and transmits the message to the next hop. The burden is on the source to 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. This approach has the advantage of requiring very little forwarding logic at intermediate nodes, and allows for entire routes to be sender authenticated using digital signatures, as in Ariadne.

F. Attacks on Stateful Protocols

Two important classes of stateful protocols are link-state and distance-vector. In link-state protocols, such as OLSR nodes keep a record of the up-or-down state of links in the network, and flood routing updates every time a link goes down or a new link is enabled.

Distance vector protocols like DSDV keep track of the next hop to every destination, indexed by a route cost metric, e.g., the number of hops. In this scheme, only routing updates that change the cost of a given route need to be propagated. Routes in link-state and distance-vector networks are built dynamically from many independent forwarding decisions, so adversaries have limited power to affect packet forwarding, making these protocols immune to carousel and stretch attacks. In fact, any time adversaries cannot specify the full path, the potential for Vampire attack is reduced. However, malicious nodes can still misforward packets, forcing packet forwarding by nodes would not normally be along packet paths. For instance, an adversary can forward packets either back toward the source if the adversary is an intermediary or to a non optimal next hop if the adversary is either an intermediary or the source.

IV. CONCLUSIONS

In this project, it defined Vampire attacks, a new class of resource consumption attacks that use routing protocols to permanently disable ad hoc wireless sensor networks by depleting nodes battery power. These attacks do not depend on particular protocols or implementations, but rather expose vulnerabilities in a number of popular protocol classes. This project showed a number of proof-of-concept attacks against representative examples of existing routing protocols using a small number of weak adversaries, and measured their attack success on a randomly generated topology of 30 nodes. Simulation results show that depending on the location of the adversary, network energy expenditure during the forwarding phase increases from between 50 to 1,000 percent. Theoretical worst case energy usage can increase by as much as a factor of O (N) per adversary per packet, where N is the network size. This project proposed defences against some of the forwarding-phase attacks and described PLGPa, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations.

ACKNOWLEDGMENT

We express our thanks to editorial board of international journal of computer science and mobile computing, for providing the essential publication and we are grateful to the chief editor **Mohammad Zainuddin M. Tech.,** as he is the leading light of this journal. We extend our deep sense of gratitude to board members and contributors of international journal of computer science and mobile computing.

REFERENCES

[1] J. Bos, D. Osvik, and D. Stefan, *"Fast Implementations of AES on Various Platforms,"* Cryptology Print Archive, 2009.

[2] J. Blaked, D. Seroussi *"Smart, Elliptic Curves in Cryptography"*, vol. 265. Cambridge Univ, 1999.

[3] H. Chan and A. Perrig, *"Security and Privacy in Sensor Networks,"* Computer, vol. 36, no. 10, pp. 103-105, Oct. 2003.

[4] J. Chang and L. Tassiulas, *"Maximum Lifetime Routing in Wireless Sensor Networks,"* IEEE/ACM Trans. Networking, vol. 12, no. 4, pp. 609-619, Aug. 2004.

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

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

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

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

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

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

[11] D.J. Bernstein, *"Syn Cookies,"* http://cr.yp.to/syncookies.html, 1996.

[12] A. Krolle, S. Fekete, D. Pfisterer, and S. Fischer, *"Deterministic Boundary Recognition and Topology Routing for Large Sensor Networks,"* Proc. Ann. ACM-SIAM Symp. Discrete Algorithms, 2006.pplications, 2003.