ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (265-270), Month: October - December 2014, Available at: www.researchpublish.com

Energy Efficient Paradigm for Multiple Localized Routing In Wireless Ad Hoc Sensor Networks

[1]S.Narmadha, [2]P.K.Mangaiyarkarasi

[1]M.C.A., Research Scholor, [2]M.C.A., M.Phil. Assistant Professor, Dept of Computer Science,
Kongu Arts and Science College, Erode, Tamil Nadu, India

Abstract: **Ad hoc low power wireless networks are an exciting research direction in sensing and preventing the environment from hackers. This thesis explores resource depletion attacks at the routing protocol layer, which permanently disable networks by quickly draining node's battery power. Carousel attack and Stretch attack are the possible scenarios occurred in this problem. The work proposes the concepts using Weight Based Synchronization, Future Peak Detection and Randomized Future Peak Detection algorithms where nodes are used to send updates to their neighbors. Weight based synchronization is used to maintain the cluster size. Future peak detection algorithm is used to calculate the average time of sending packets from source to destination with the help of relative time of their sender's next transmission. This allows nodes to save battery power in network without missing updates from their neighbors.**

Keywords**: Node's battery power, Applications, Distributed system, Synchronization.**

I. INTRODUCTION

Wireless communication has become of such fundamental importance that a world without it is no longer imaginable for many of us. Beyond the established technologies such as mobile phones and WLAN, new approaches to wireless communication are emerging. One of them are so called ad hoc and sensor networks. Ad hoc and sensor networks are formed by autonomous nodes communicating via radio without any additional backbone infrastructure. Typically, if two nodes are not within mutual transmission range, they communicate through intermediate nodes relaying their message, the communication infrastructure is provided by the devices themselves.

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, environment. Recently, wireless sensor networks have been attracting a great deal of commercial and research interest. In particular, practical emergence of wireless ad-hoc networks is widely considered revolutionary both in terms of paradigm shift as well as enabler of new applications. In ad-hoc networks there is no fixed network infrastructure (such as in cellular phone networks) and therefore they can be deployed and adapted much more rapidly.

Furthermore, integration of inexpensive, power efficient and reliable sensors in nodes of wireless ad-hoc networks, with significant computational and communication resources, opens new research and engineering vistas.

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.

Attacks on Sensor Network Routing:

Many sensor network routing protocols are quite simple, and for this reason are sometimes even more susceptible to attacks against general ad-hoc routing protocols. Most network layer attacks against sensor networks fall into one of the following categories.

- Spoofed, altered, or replayed routing information
- Selective for wardings
- Sinkhole attacks
- Sybil attacks

II. LITERATURE REVIEW

A. 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. According to Imad Aad and Jean Pierre Hubaux [1], 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.The goal of JF nodes is to reduce the goodput of all traversing flows to near-zero while dropping zero or a small fraction of packets. In particular, JF nodes employ one of two 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 [14]. However, no TCP variant is robust to malicious and persistent reordering as employed by the JF misordering attack. The second JF mechanism is periodic dropping according to a maliciously chosen period. This attack is inspired by the Shrew attack[5], in which an endpoint sends maliciously spaced periodic pulses in order to force flows into repeated timeout phases.

B. Provably Secure On-Demand Source Routing In Mobile Ad Hoc Networks:

According to Gergely Acs and Istvan Vajda[2], 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 “secure” routing protocol [10].

These attacks clearly demonstrate that flaws can be very subtle, and therefore, hard to discover by informal reasoning[22]. Hence, they advocate a more systematic approach to analyzing ad hoc routing protocols, which is based on a rigorous mathematical model, in which precise definitions of security can be given, and sound proof techniques can be developed.

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. Another type of classification distinguishes routing table based protocols (e.g., AODV) and source routing protocols (e.g., DSR).

C. Dos-Resistant Authentication with Client Puzzles:

According to Tuomas Aura and Pekka Nikande[3], Denial-of-service (DOS) attacks that exhaust the server's resources are a growing concern on the Internet and other open communications systems. For example, in the SYN attack, a client floods the server with the opening messages of the TCP protocol and fills the space reserved in the server for storing half-open connections.

In this paper [3], author advocates the design principle that the client should always commit its resources to the authentication protocol first and the server should be able to verify the client commitment before allocating its own resources. The rule of thumb is that, at any point before reliable authentication, the cost of the protocol run to the client should be greater than to the server. The server should remain stateless and refuse to perform expensive cryptographic operations until it has verified the client's solution to a puzzle. It should be noted, however, other techniques are needed to protect individual clients against denial of service and to prevent exhaustion of communications bandwidth.

D. 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. According to Sheetalkumar Doshi and Timothy X Brown [9], 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. Traditional communication theory focuses on physical and link layer mechanisms for reducing energy consumption. Here they explore minimum energy routing protocols. Efficient minimum energy routing schemes can greatly reduce energy consumption and lead to a longer battery life of the device. Ad hoc routing protocols can be broadly classified as table driven routing protocols and source initiated on- demand routing protocols [19].

E. An Energy Consumption Model For Performance Analysis Of Routing Protocols For Mobile Ad Hoc Networks:

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.

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. According to *Laura Marie* Feeney[11], develops the hypothesis that resource utilization in MANET protocols is not fully addressed by evaluations which consider only the bandwidth used in route negotiation. By examining energy consumption, one can identify both costly protocol behaviors and link-layer issues that take on particular importance in the ad hoc environment. Link-layer costs associated with the ad hoc environment are potentially extremely significant.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 2, Issue 4, pp: (265-270), Month: October - December 2014, Available at: www.researchpublish.com

III. PROBLEM DESCRIPTION

Carousel Attack and Stretch Attack:

In routing schemes, directional antenna and worm-hole attacks can be used to deliver packets to multiple remote network positions, forcing packet processing at nodes that would not normally receive that packet at all, and thus increasing network wide energy expenditure.

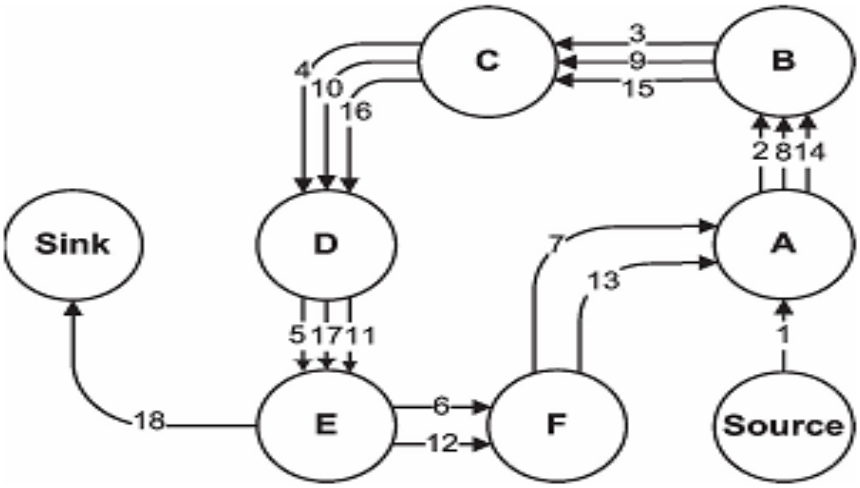

Fig. 1.1 Malicious Route Carousel Attacks On Source Routing

In this first attack, an adversary composes packets with purposely introduced routing loops is know as carousel attack, since it sends packets in circles as shown in Fig. 1.1. 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.

In this second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network called as stretch attack, since it increases packet path lengths, causing packets to be processed by a number of nodes that is independent of hop count along the shortest path between the adversary and packet destination. A solution to such threats is to authenticate the client before the server commits any resources to it. The authentication, however, creates new opportunities for DOS attacks because authentication protocols.

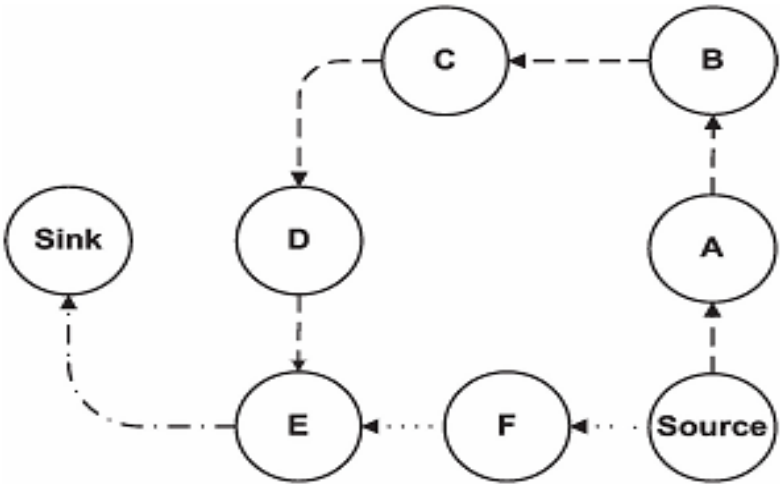

Fig. 1.2 Malicious Route Stretch Attacks On Source Routing

An example is illustrated in Fig. 1.2. Results show that in a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node.

IV. PROBLEM DEFINITION

This thesis had no-backtracking property, since it holds if and only if a packet is moving strictly closer to its destination with every hop, and it mitigates all mentioned Vampire attacks with the exception of malicious flooded discovery, which is significantly harder to detect or prevent.

This thesis evaluated both the carousel and stretch attacks ,a randomly generated node topology and a single randomly selected malicious DSR agent. Energy usage is measured for the minimum number of packets required to deliver a single message, so sending more messages increases the strength of the attack linearly until bandwidth saturation In other words, malicious nodes are not driving down the cumulative energy of the network purely by their own use of energy.

Nevertheless, malicious node energy consumption data are omitted for clarity. The attacks are carried out by a randomly selected adversary using the least intelligent attack strategy to obtain average expected damage estimates. In addition to Vampire attack, Inflation attack is also prevented.

- Weight based synchronization is works with correct weight information chooses the correct cluster for the given node.
- Future peak detection algorithm 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.

V. SYSTEM METHODOLOGY

To implement the Weight Based Synchronization algorithm to find the winner slot to store the packet data.

- To extend the Weight Based Synchronization algorithm and implement the Future Peak Detection algorithm to avoid the inflation attack which is made by sending false maximum weight among the nodes.
- To extend the Future Peak Detection algorithm and implement the Randomized Future Peak Detection algorithm to synchronize all the neighbor nodes by using all the slots.

VI. CONCLUSION

Ad hoc networking is a promising but challenging emerging technology. 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. 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, scalable and efficiently defend against attacks.

The application works well for given tasks in windows environment. The system eliminates the difficulties in the existing system. It is developed in a user-friendly manner. The system is very fast and any transaction can be viewed or retaken at any level.

VII. FUTURE ENHANCEMENTS

The protocols are computationally inexpensive, provide significant battery savings, are scalable and efficiently defend against attacks.It can be utilized for deploying applications in real life environments. Some other effective technique can be used for periodic transmissions of nodes, which allows nodes to save battery power. To save the battery power in network without missing updates from their neighbors.

REFERENCES

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

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

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

[4] Armstrong.T, "Wake-Up Based Power Management in Multi- Hop Wireless Networks," Term Survey Paper for QoS Provisioning in Mobile Networks, 2005.

[5] Bos.J.W, Osvik.D.A, and Stefan.D , "Fast Implementations of AES on Various Platforms," Cryptology ePrint Archive, Report 2009/ 501, http://eprint.iacr.org, 2009.

[6] Chang.J., Tassiluas.L., "Energy Conserving Routing in Wireless Ad-Hoc Networks," Proceedings of IEEE INFO-COM 2000, pp. 22-31, 2000.

[7] Chen.B, Jamieson, K. Balakrishnan, H. Morris, R,Span, "An Energy-Efficient Coordination Algorithm for Topology Maintenance in Ad Hoc Wireless Networks", Proceedings of MOBICOM 2001, 2001.

[8] Deng.J, Han.R, and Mishra.S, "INSENS: Intrusion-Tolerant Routing for Wireless Sensor Networks," Computer Comm., vol. 29, no. 2, pp. 216-230, 2006.

[9] Doshi.S, Bhandare.S, and Brown T.X, "An On-Demand Minimum Energy R outing Protocol for a Wireless Ad Hoc Network," ACM SIGMOBILE Mobile Computing and Comm. Rev., vol. 6, no. 3, pp. 50-66, 2002.