IOSR Journal of Computer Engineering (IOSR-JCE)
e-ISSN: 2278-0661, p- ISSN: 2278-8727Volume 16, Issue 3, Ver. III (May-Jun. 2014), PP 97-101
www.iosrjournals.org

A Study of vampire Attack to Avoid the Intruders without Backtracking Method

[1]M.Mohana Priya, [2]Ms.J.Emi Karmichael M.Tech
[1]II ME (CSE), Shivani Engineering College, Trichy
[2]Asst.Professor (CSE), Shivani Engineering College,Trichy

Abstract*: In a Wireless sensor network, every hub gathers the information and transmits all the information parcels to the sink hub utilizing any directing conventions. The directing Protocols are intended to be secure and absence of insurance from the different assaults. The vampire ambushes are not particular to any particular conventions and additionally exceptionally troublesome to catch and keep the assaults. Another plan to deactivate them by effectively distinguishing all assaulter hubs. A versatile force multicast calculation strategy can fill in as a requisition layer administration and profit numerous existing receptive sticking safeguarding plans. DDos ambush administration system for questionable remote sensor systems. It furnishes an enhanced calculation concerning two complex ambushes models, with a specific end goal to upgrade its power for different system situations. What's more additionally give a no Backtracking technique to evade the bundle misfortune.*

Keywords: *Wireless Sensor Network, Vampire attack, Adaptive power multicast, DDOs*

I. Introduction

1. Denial Of Service Attack

A denial-of-service attack DoS attack or distributed denial-of-service attack is an attempt to make a machine or 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.

Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name servers. This technique has now seen extensive use in certain games, used by server owners, or disgruntled competitors on games. Increasingly, DoS attacks have also been used as a form of resistance. DoS they say is a tool for registering dissent. Richard Stallman has stated that DoS is a form of 'Internet Street Protests'. The term is generally used relating to computer networks, but is not limited to this field; for example, it is also used in reference to CPU resource management.

A DoS attack may include execution of malware intended to:

- Max out the processor's usage, preventing any work from occurring.
- Trigger errors in the microcode of the machine.
- Trigger errors in the sequencing of instructions, so as to force the computer into an unstable state or lock-up.
- Exploit errors in the operating system, causing resource starvation and/or thrashing, i.e. to use up all available facilities so no real work can be accomplished or it can crash the system itself
- Crash the operating system itself.

2. Vampire 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.

3. Stateless Protocols

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 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. It independently computed resource utilization of honest and malicious nodes and found that malicious nodes did not use a disproportionate amount of energy in carrying out the attack. 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.

4. Carousel Attack

In this 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. An example of this type of route malicious node 0 carries out a carousel attack, sending a single message to node 19 which does not have to be malicious. Note the drastic increase in energy usage along the original path. Assuming the adversary limits the transmission rate to avoid saturating the network, the theoretical limit of this attack is an energy usage increase factors of O (N) where the maximum route length is. Overall energy consumption increases by up to a factor of 3.96 per message. On average, a randomly located carousel attacker in our example topology can increase network energy consumption by a factor of 1:48 to 0:99. The reason for this large standard deviation is that the attack does not always increase energy usage the length of the adversarial path is a multiple of the honest path, which is in turn, affected by the position of the adversary in relation to the destination, so the adversary's position is important to the success of this attack. 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.

5. Stretch Attack

Another attack in the same vein is the 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 network-wide energy consumption in the presence of a single randomly selected Vampire in terms of the maliciousness of the adversary, or the induced stretch of the optimal route in number of hops. Increasing maliciousness beyond nine has no effect due to the diameter of our test topology. Network links become saturated at 10,000 messages per second even without the stretch attack, but the adversary can achieve the same effects by sending an order of magnitude fewer messages at a stretch attack maliciousness level of 8 or greater. This reduces cumulative network energy by 3 percent, or almost the entire lifetime of a single node. Therefore, the stretch attack increases the effectiveness of an adversary by an order of magnitude, reducing its energy expenditure to compose and transmits messages.

6. Stateful Protocols

It move on to stateful routing protocols, where network nodes are aware of the network topology and its state, and make local forwarding decisions based on that stored state. 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 fact, any time adversaries cannot specify the full path, the potential for Vampire attack is reduced. However, malicious nodes can still forwarded packets, forcing packet forwarding by nodes that would not normally be along packet paths.

7. Malicious Discovery Attack

Another attack on all previously mentioned routing protocols including stateful and stateless is spurious route discovery. In most protocols, every node will forward route discovery packets and sometimes route responses as well, meaning it is possible to initiate a flood by sending a single message. Systems that perform as-needed route discovery are particularly vulnerable, since nodes may legitimately initiate discovery at any time, not just during a topology change. A malicious node has a number of ways to induce a perceived topology change: it may simply falsely claim that a link is down, or claim a new link to a nonexistent node.

II. Literature Survey

2.1 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. These attacks clearly demonstrate that flaws can be very subtle, and therefore, hard to discover by informal reasoning. It proposes a mathematical framework in which security can be precisely defined, and routing protocols for mobile ad hoc networks can be analyzed rigorously. In framework is tailored for on-demand source routing protocols, but the general principles are applicable to other types of protocols too. Regarding the capabilities of the adversary, 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

2.1.1 Drawbacks

A problem with the protocol, and often, one can construct an attack by looking at where the proof failed. Many researchers, and several “secure” routing protocols have been proposed for ad hoc networks. However, the securities of those protocols have been analyzed either by informal means only, or with formal methods that have never been intended for the analysis of this kind of protocols. These attacks clearly demonstrate that flaws can be very subtle, and therefore, hard to discover by informal reasoning. Consequently, it is also difficult to gain sufficient assurances that a protocol is free of flaws. The approach of verifying the protocol for a few numbers of specific configurations can never be exhaustive, and thus, it is far from being satisfactory as a method for security analysis.

2.2fast Implementations Of Aes On Variousplatforms

Target platforms are 8-bit AVR microcontrollers, NVIDIA graphics processing units and the Cell broadband engine. The new AVR implementation requires 124.6 and 181.3 cycles per byte for encryption and decryption with a code size of less than two kilobyte. As the outcome of a public competition, Rijndael was announced as the Advanced Encryption Standard by the US National Institute of Standards and Technology. The byte-sliced implementation for the synergistic processing elements of the Cell architecture achieves speed of 11.7 and 14.4 cycles per byte for encryption and decryption. The other target platforms, the Cell and the GPU, are chosen because of their ability to process many streams simultaneously, using single instruction, multiple data and single instruction, multiple threads techniques respectively.

2.2.1 Drawbacks

That although direct addressing can access the whole data space, indirect addressing with displacement is limited to 63 address locations from only one of the pointer registers, and this restriction may require the implementer to use techniques such as double-jumping. Another limitation is that only the Z register may be used for addressing ash memory, e.g., for AES S-box lookups, and in some AVR devices this is not possible at all.

2.3denial Of Service Resilience In Ad Hoc Networks

Significant progress has been made towards making ad hoc networks secure and DoS resilient. There remains an indefinite “arms race” in system and protocol design: attackers or researchers anticipating the moves of attackers will continually introduce increasingly sophisticated attacks, and protocol designers will continually design protocol mechanisms designed to thwart the new attacks. It design and study DoS attacks in order to assess the damage that difficult to detect attackers can cause. 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.

2.3.1 Drawbacks

However, no TCP variant is robust to malicious and persistent reordering as employed by the JF disordering attack. The second JF mechanism is periodic dropping according to a maliciously chosen period. Intuitively, if a system has no mobility and infinite route lifetimes JF will have little effect as nodes will eventually discover routes without JF if such routes exist. However, as mobility increases, the route lifetime shortens and the effects of JF become increasingly pronounced as the time spent uselessly transmitting on JF paths and re-establishing routes becomes an increasing fraction of a flow’s lifetime. Thus, an analytical and experimental relationship that characterizes the impact of these timescales on flow good put.

2.4 New Aes Software Speed Record

The new speed records for AES software, taking advantage of architecture-dependent reduction of instructions used to compute AES and microarchitecture-dependent reduction of cycles used for those instructions .Almost all of the specific techniques it use are well known. The main novelty lies in the analysis and combination of these techniques, producing surprisingly high speeds for AES. There are also, in the literature, many different ways to benchmark AES software. This variability interferes with comparisons.

2.4.1 Drawbacks

First, some applications en- crypt long streams and do not mind padding to 2048-byte boundaries; second, some applications will use bits licing on both client and server and can thus eliminate the costs of transposition; third, bits liced implementations are inherently immune to the cache-timing attacks.

2.5dos-Resistant Authentication With Client Puzzles

Public-key authentication does not completely protect against the attacks because the authentication protocols often leave ways for an unauthenticated client to consume a server's memory space and computational resources by initiating a large number of protocol runs and inducing the server to perform expensive cryptographic computations. 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 usually require the server to store session-specific state data, such as nonce, and to compute expensive public-key operations. It shows how stateless authentication protocols and the client puzzles of Juels and Brainard can be used to prevent such attacks.

2.5.1 Drawbacks

The protocol is that the route maintenance mechanism does not locally repair a broken link. Stale route cache information could also result in inconsistencies during the route reconstruction phase. The connection setup delay is higher than in table-driven protocols. Even though the protocol performs well in static and low-mobility environments, the performance degrades rapidly with increasing mobility. Also, considerable routing overhead is involved due to the source-routing mechanism employed in DSR. This routing overhead is directly proportional to the path length.

III. Methodology

To enhance the performance robustness of the system, under base station failure events, it extends the basic algorithm by introducing an opportunistic relay aided multicasting operation. Under the extended multicasting protocol, in addition to using base stations to multicast messages to nodes that are located closer to them, mobile stations can be elected to relay multicast messages that they have received directly from their base stations to peripheral nodes in their neighborhood. It shows that this extended adaptive power and rate multicasting scheduling algorithm is effective in adapting to a failure of a base station node, limiting the performance degradation that is incurred. For an illustrative scenario, the extended relay aided scheme is noted to yield a throughput rate that is higher than that attained by a scheme that doesn't employ relay nodes by about 20%, while consuming less energy resources.

IV. Conclusion

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. They 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.

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.

V. Future Enancement

Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks. DDoS attacks cannot be detected effectively by traditional methods in time, a DDoS attack detecting algorithm based on the relation of characteristic parameters is researched according to the analysis of the essential characteristic of DDoS. The scheme can detect DDoS attack traffic in its early stages when the attacking packet's attribute value has no distinct features. It can differentiate DDoS from normal flash crowd traffic.

References

[1]. Eugene Y. Vasserman and Nicholas Hopper, In 2013, Vampire Attacks: Draining Life from Wireless Ad Hoc Sensor Networks.

[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-Demand Source Routing in Mobile Ad Hoc Networks,” IEEE Trans. Mobile Computing, vol. 5, no. 11, pp. 1533-1546, Nov. 2006.

[4]. T. Aura, “Dos-Resistant Authentication with Client Puzzles,” Proc. Int’l Workshop Security Protocols, 2001.

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

[6]. D. Bernstein and P. Schwabe, “New AES Software Speed Records,” Proc. Ninth Int’l Conf. Cryptology in India: Progress in Cryptology (INDOCRYPT), 2008.

[7]. I.F. Blaked, G. Seroussi, and N.P. Smart, Elliptic Curves in Cryptography, vol. 265. Cambridge Univ, 1999.