International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

MANET Approach for Analysis of Network Bandwidth Monitoring System

[a]*Dr.B. Firdaus begam*, [b]*A.Sriram,*

[a]Assistant Professor, Department of Computer Science, Karpagam Academy of Higher Education
[b]Department of Computer Science, Karpagam Academy of Higher Education

ABSTRACT

Most of the organization they connect more numbers of systems to form a network to make their work easier to share their files and folders. While connecting we want to monitor the network system activities for secure purpose. This Paper deals with monitoring the Network Screen Activities with bandwidth details. It has two methodologies one for Client and another for Server. In the proposed system we introduce current session option to monitor the network bandwidth at the same time and in the accesses folder option shows the username and accessed folders. The proposed project is aimed to monitor the traffic and to route the network traffic so that at any particular node, or route, the congestion does not occur. ttcp is installed on two machines – one will be the sender, the other the receiver. The receiver is started first and waits for a connection. Once the two connect, the sending machine sends data to the receiver and displays the overall throughput of the network they traverse. The amount of data sent and other options are configurable through command line parameters. The statistics output covers TCP/UDP payload and is generally displayed by default in KiB/s (kibiBytes per second) instead of kb/s (kilobits per second), but it can be configured to be displayed in other ways on some implementations. The reported throughput is more accurately calculated on the receive side than the transmit side. Since the transmit operation may complete before all bytes actually have been transmitted.

Keywords: TCP/IP, WSN, Routing Algorithm

1. 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 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. 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. Methodology

This paper makes three primary contributions. 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 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 behavior and cannot optimize out malicious action. Second, we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire (insider adversary). Third, we modify an existing sensor network routing protocol to provably bound the damage from Vampire attacks during packet forwarding.

A. Network Creation Module

In this Module, we setup our Network model with Sink, Source and with nodes namely Node A, B, C, D, E, F. Each node will be assigned unique Identity number. And also 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. The user, 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.

B. Stretch attack Module

In our second attack, also targeting source routing, an adversary constructs artificially long routes, potentially traversing every node in the network. We call this the 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. An example is illustrated in Fig. 1b. Results show that in a randomly generated topology, a single attacker can use a carousel attack to increase energy consumption by as much as a factor of 4, while stretch attacks increase energy usage by up to an order of magnitude, depending on the position of the malicious node. The impact of these attacks can be further increased by combining them, increasing the number of adversarial nodes in the network, or simply sending more packets. Although in networks that do not employ authentication or only use end-to-end authentication, adversaries are free to replace routes in any overheard packets, we assume that only messages originated by adversaries may have maliciously composed routes.

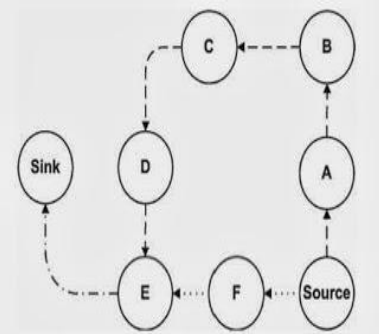

Fig-1 Stretch Attack module

C. Secured Transmission Module

In this module, we show the secured transmission done in the nodes by overcoming the vampire attacks. Where the data travels in the honest route and mitigating the vampire attacks. It performs Encrypt Data and sends the result to the destination. The data are transmitting with secured manner.

D. 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. First extracts individual receiver data by decrypting the cipher text. Afterward, the receiver verifies the authenticity and integrity of the decrypted data based on the corresponding node.

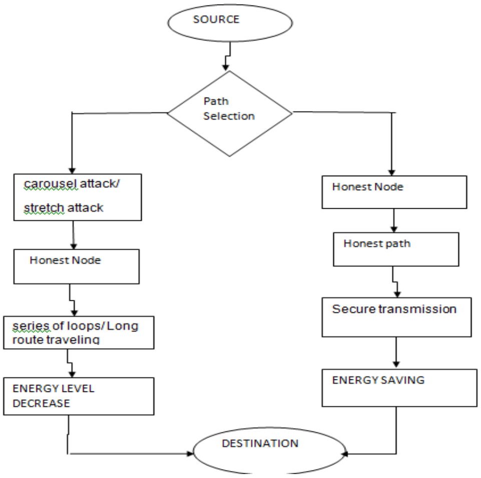

Fig-2 System Architecture

3. Results and Discussion

In proposed system we show simulation results quantifying the performance of several representative protocols in the presence of a single Vampire. Then, we modify an existing sensor network routing protocol to provably bind the damage from Vampire attacks during packet forwarding.

4. Conclusion

We 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. We 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. In this paper, we 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. We 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 per adversary per packet, where N is the network size. We proposed defenses against some of the forwarding-phase attacks and described PLGP, the first sensor network routing protocol that provably bounds damage from Vampire attacks by verifying that packets consistently make progress toward their destinations. We have not offered a fully satisfactory solution for Vampire attacks during the topology discovery phase, but suggested some intuition about damage limitations possible with further modifications to PLGP. Derivation of damage bounds and defenses for topology discovery, as well as handling mobile networks, is left for future work.

REFERENCES

1. “Head First Servlets java and JSP: Passing the Sun Certified Web Component Developer Exam “, by Bryan Basham (Author), Kathy Sierra (Author), Bert Bates (Author), O'Reilly Media; Second Edition edition (April 1, 2008).

2. “Core Java™, Volume I--Fundamentals (8th Edition) “ , by Cay S. Horstmann, Prentice Hall; 8 edition (April 18, 2008).

3. http://www.jsp.net/

4. http://www.tutorialspoint.com/mysql/

5. http://www.javatpoint.com/java-tutorial

6. http://www.w3schools.in/java-tutorial/

7. M. Aal-Nouman, H. Takruri-Rizka, M. Hope, “Transmission Of Medical Messages Of Patient Using Control Signal Of Cellular Network”, Telematics And Informatics, Https://Doi.Org/10.1016/J.Tele.2017.11.008, 2017

8. M Praneesh and Jaya R Kumar. Article: Novel Approach for Color based Comic Image Segmentation for Extraction of Text using Modify Fuzzy Possiblistic C-Means Clustering Algorithm. IJCA Special Issue on Information Processing and Remote Computing IPRC(1):16-18, August 2012. Published by Foundation of Computer Science, New York, USA.