Sleuthing Wormhole Attacks Using Hidden Markov Model in Wireless Networks

Sunitha M, Priyadharshini P, CSE Department, GRT Institute of Engineering and Technology, Tiruttani

***Abstract*---- Wireless networks are vulnerable to many attacks such as attacks like eavesdropping, man-in-the-middle etc. Therefore, security assailability should be identified and safeguard against wireless networks.We bring out the wormhole attack, a severe attack in wireless networks that is particularly challenging to protect against. The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. In the wormhole attack, an attacker captures packet at one location in the network, tunnels them to another location, and retransmits them there into the network. To struggle against wormhole attacks, we propose an anomaly-based detection system by using strategically distributed monitoring stubs (MSs).The MSs, by sniffing the traffic, extract features for detecting these attacks and construct normal usage behavior profiles. We have used a model called, Hidden Markov Model (HMM), to compute behavioral distance in order to compare the normal usage behavioral profiles to detect intrusions. The monitoring stubs produces sound alarm on the sender side when data gets attacked.**

Keywords *– Wormhole attack, Mobile Ad hoc Network, Security, Intrusion detection.*

I. INTRODUCTION

Network security consists of the provisions and policies adopted by a network administrator to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator. Users choose or are assigned an ID and password or other authenticating information that allows them access to information and programs within their authority. Network security covers a variety of computer networks, both public and private, that are used in everyday jobs conducting transactions and communications among businesses, government agencies and individuals. Networks can be private, such as within a company, and others which might be open to public access. Network security is involved in organizations, enterprises, and other types of institutions.

Network security starts with authenticating the user, commonly with a username and a password.Once authenticated, a firewall enforces access policies such as what services are allowed to be accessed by the network users. Though effective to prevent unauthorized access, this component may fail to check potentially harmful content such as computer worms or Trojans being transmitted over the network. Anti-virus software or an intrusion prevention system (IPS) help detect and inhibit the action of such malware. An anomaly-based intrusion detection system may also monitor the network and traffic for unexpected (i.e. suspicious) content or behavior and other anomalies to protect resources, e.g. from denial of service attacks. Suppose a strange man is standing in front of your house. He looks around, studying the surroundings, and then goes to the front door and starts turning the knob. The door is locked. He moves to a nearby window and gently tries to open it. It, too, is locked. It seems your house is secure. So why install an alarm.

II. TYPES OF INTRUSION DETECTION SYSTEM

2.1. *Network Intrusion Detection System (NIDS)*

Network Intrusion Detection System (NIDS) is an intrusion detection system that attempts to discover unauthorized access to a computer network by analyzing traffic on the network for signs of malicious activity. Network intrusion detection systems gain access to network traffic by connecting to a network hub, network switch configured for port mirroring, or network tap.

2.2 *Host-Based Intrusion Detection System (HIDS)*

A host-based intrusion detection system (HIDS) is an intrusion detection system that monitors and analyzes the internals of a computing system as well as the network packets on its network interfaces.

2.3. *Stack-Based Intrusion Detection System (SIDS)*

This type of system consists of an evolution to the HIDS systems. The packets are examined as they go through the TCP/IP stack and, therefore, it is not necessary for them to work with the network interface in promiscuous mode.

III. RELATED WORK

The Internet and computer networks are exposed to an increasing number of security threats. With new types of attacks appearing continually, developing flexible and adaptive security oriented approaches is a severe challenge. Garcia-Teodoro et al [1]. Describes the most well-known anomaly-based intrusion detection techniques, available platforms, systems under development and research projects in the area are presented. The authors discusses the foundations of the main A-NIDS technologies, together with their general operational architecture, and provides a classification for them according to the type of processing related to the ''behavioural'' model for the target system. Another valuable aspect of studying this paper is that it describes, in a concise way, the main features of several currently available IDS systems/ platforms. Finally, the most significant open issues regarding A-NIDS are identified, among which that of assessment is given particular emphasis. The information presented in this paper constitutes an important starting point for addressing R&D in the field of IDS.

Some work has been done to detect wormhole attacks. Most of them based on the fact that transmission time between two wormhole nodes or between two fake neighbors is much longer than that between two real neighbors which are close together. Because two wormhole nodes (or two fake neighbors) are far from each other and packets sent between two wormhole nodes may be go through several intermediate nodes so it takes a longer time to transmit a packet between two wormhole nodes (or two fake neighbors) than between two real neighbors which are close together. By detecting this difference, we can identify wormhole attacks.

Yih-chun hu et al [2]. Introduced the notion of a packet leash as a general mechanism for detecting and thus defending against wormhole attacks. A leash is any information that is added to a packet designed to restrict the packet's maximum allowed transmission distance. We distinguish between geographicalleashes and temporal leashes. A geographical leash ensures that the recipient of the packet is within a certain distance from the sender. A temporal leash ensures that the packet has an upper bound on its lifetime, which restricts the maximum travel distance, since the packet can travel at most at the speed of light. Either type of leash can prevent the wormhole attack, because it allows the receiver of a packet to detect if the packet traveled further than the leash allows.

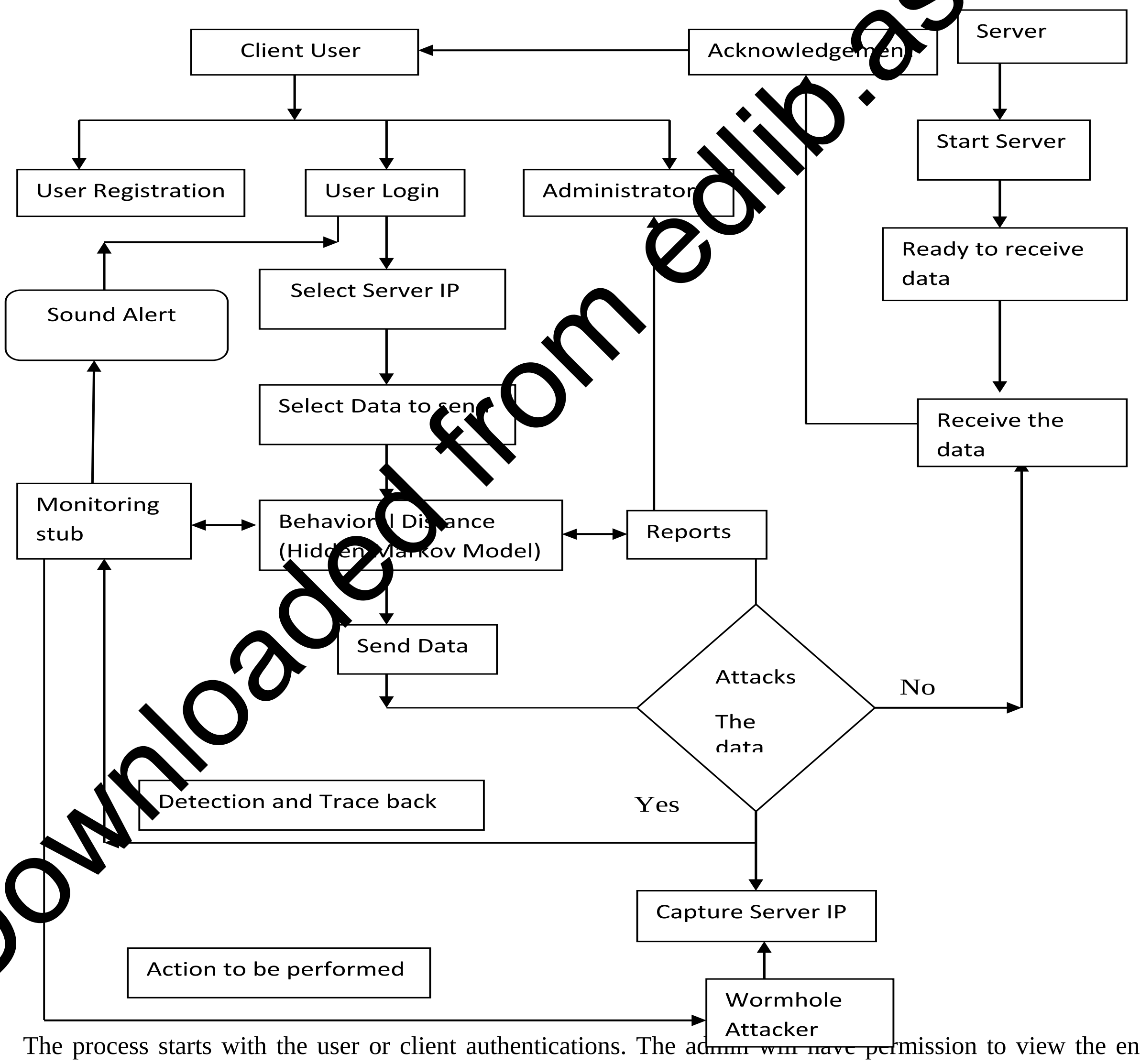
The authors presented the design and operation of protocol which is named TIK. This TIK protocol is used to implement the temporal leashes. TIK stands for TESLA with Instant Key disclosure, and is an extension of the TESLA broadcastauthentication protocol. The author then described several stages of the TIK protocol. Finally the author evaluate the performance of the TIK protocol and compare the geographical and temporal leashes which shows geographic leashes are less efficient than temporal leashes.In order to avoid using special hardware, Jane Zhen and Sampalli Srinivas introduced a mechanism called Round Trip Time (RTT) to detect wormhole between two nodes. In this paper the authors classified the wormhole attacks into two categories namely hidden and exposed attacks. A node, say A, calculates the RTT with another node, say B, by sending a message to node B requiring an immediate reply from B. The RTT between A and B is the time between A's sending the request message and receiving the reply message from B. In this mechanism each node (called N) will calculate the RTT between N and all N's neighbors.

Because the RTT between two fake neighbors is higher than that between two real neighbors so by comparing these RTTs between A and A's neighbors, node A can identify which neighbors are fake neighbors and which neighbors are real neighbors. This mechanism do not require any special hardware and easy to implement but it cannot detect exposed attacks because no fake neighbor is created in exposed attacks.

In order to overcome the above problem Hon Sun Chiu and King-Shan Lui [4] proposed another mechanism called DelPHI (Delay Per Hop Indicator), which is able to detect both hidden and exposed wormhole attacks. In this mechanism, the authors tried to find every available disjoint path between a sender and a receiver. Then, they calculate delay time & length of each path, computing Delay Per Hop value (average delay time per hop along each path). Delay per Hop values of paths are used to identify wormhole: the path containing wormhole link will have greater Delay Per Hop value. This mechanism can detect both kind of wormhole but they cannot pinpoint the wormhole location. Moreover, because lengths of paths are changed by every node (including wormhole nodes) so wormhole nodes could change the path length in a certain way to make them unable to be detected.

There are several other approaches which do not use transmission time to detect wormhole. Levente et al [5]. two statistical approaches to detect wormhole attack in Wireless Ad Hoc Networks namely Neighbor Number Test and All Distance Test. The Neighbor Number Test bases on a simple assumption that a wormhole will increase the number of neighbors of the nodes (fake neighbors) in its radius. The base station will get neighborhood information from all sensor nodes, computes the hypothetical distribution of the number of neighbors and uses statistical test to decide if there is a wormhole or not. An All Distance Test detects wormhole by computing the distribution of the length of the shortest paths between all pairs of nodes. In these two algorithms, most of the workload is done in the base station to save sensor nodes' resources. However, one of the major drawbacks is that they cannot pinpoint the location of wormhole which is necessary for a successful defense. This is corresponding to the observation values generated by the states of hidden Markov models. So complicate network attacks can be described by hidden Markov models. Each attack step is corresponding to a state of hidden Markov models. The transition of attack steps is corresponding to the transition between the states of hidden Markov models.

IV. SYSTEM ARCHITECTURE



The process starts with the user or client authentications. The admin will have permission to view the entire processes done by the user. The user can only view the authenticated page after getting registered to the approach. User can view their personal information and the data which sent by him. In the server module have the static and secure login to enter and receive the data starts the server to. The network has divided by workgroups. This will help us to get the connected and the active systems in the network. After getting login to our process, this will get the connected systems and shows to the users. The user can select the system to deliver their data by file transfer. The disconnected and the shutdown systems are to transfer the data and the file to be transferred. The selected file will be encrypted for secured transfer. When the data received by the desired path of destination, the key automatically enabled and decrypted. When the user starts the process, the monitoring stub will initiate automatically to find behavioral distance and the evolutionary distances. In our process, we have to monitor the client data, which are sent to the receiver with a certain path. After the intruder affects the current data, there is no use of reports. So here, we trace back the path of every data information.Tracing the path of the data from one end to another end. when the data information path getting differ from the desired paths.

V. METHODOLOGY

Wireless networks are vulnerable to many attacks such as attacks like eavesdropping, man-in-the-middle, etc. Therefore, security assail ability in wireless networks should be identified and safeguard against. In this paper, we bring out the wormhole attack, a severe attack in wireless networks that is particularly challenging to protect against. The wormhole attack is very powerful, and preventing the attack has proven to be very difficult. In the wormhole attack, an attacker records packet at one location in the network, tunnels them to another location, and retransmits them there into the network. The wormhole attack can form a serious threat in wireless networks without some mechanism to protect against the wormhole attack, would be unable to find routes longer than one or two hops, severely interrupting communication.

Wormhole attacks, we propose an anomaly-based detection system by using strategically distributed monitoring stubs (MSs).The MSs, by sniffing the traffic, extract features for detecting these attacks and construct normal usage behavior profiles. Upon detecting suspicious activities due to the deviations from these normal profiles, the MSs notify to struggle against the victim servers, which may then take necessary actions. In addition to detecting attacks, the MSs can also trace back the originating network of the attack.

In this paper we have applied a model called Hidden Markov Model (HMM), to compute the behavioral distance in order to compare the normal usage behavioral profiles to detect intrusions. The monitoring stubs produces sound alarm on the sender side when data gets attacked.

The unbridled growth of the Internet and the network-based applications has contributed to enormous security leaks. Even the cryptographic protocols, which are used to provide secure communication, are often targeted by diverse attacks. Intrusion detection systems (IDSs) are often employed to monitor network traffic and host activities that may lead to unauthorized accesses and attacks against vulnerable services. Most of the conventional misuse-based and anomaly-based IDSs are ineffective against attacks targeted at encrypted protocols since they heavily rely on inspecting the payload contents.

Fight against wormhole attacks on encrypted protocols; we propose an anomaly-based detection system by using strategically distributed monitoring stubs (MSs). We have introduced one type of attack called wormhole attacks against cryptographic protocols. The MSs, by sniffing the encrypted traffic, extract features for detecting these attacks and construct normal usage behavior profiles. Upon detecting suspicious activities due to the deviations from these normal profiles, the MSs notify the victim servers, which may then take necessary actions. In addition to detecting attacks, the MSs can also trace back the originating network of the attack.

Cryptographic protocols rely upon encryption to provide secure communication between involved parties. Secure Socket Layer (SSL) and its successor Transport Layer Security (TLS) are extensively used to provide authentication and encryption in order to transmit sensitive data. The purpose of all these encrypted protocols is to resist malicious intrusions and eavesdropping. The number of attacks against encrypted protocols has increased significantly in recent times.

With the evolution of high-speed Internet and processing power, it is only natural to assume that more sophisticated attacks will emerge and pose serious threats to encrypted protocols. In a distributed detection mechanism that is able to detect the anomalous events as early as possible, especially before significant damage is inflicted on the victim by the attacker. The coordination of distinct agents monitoring the network flows at different points requires an appropriated architecture that must be developed. We address these issues in our project effectively and attempt to design adequate solutions to these problems.

We propose a model called Hidden Markov Model which is not limited to constructing a defensive mechanism to discover wormhole attacks; we devise an aggressive countermeasure that not only detects a potential threat, but also investigates the root of the threat by attempting to trace back the attacker’s network or sub network.

Monitoring stub will helps to improve the efficiency of the trace back mechanism and also identifying the paths. Behavioral distance used to find out the hacking of information before the data corrupted or updated by the intruder. Behavioral distance is calculated by using Hidden Markov Model. Fighting against attacks on encrypted protocols in the wireless network environment. The proposed detection scheme manages to avoid false alarms when the flash crowd occurred.

We present an approach based on a novel Hidden Markov Model (HMM) for computing behavioral distance, and present the design, implementation, and evaluation of a novel architecture using HMM-based behavioral distance to detect attacks. An HMM models a doubly stochastic process; there is an underlying stochastic process that is not observable (it is "hidden") but that influences another that produces a sequence of observable symbols. When applied to our problem of computing behavioral distance, the observed symbols are process behaviors, and the hidden states correspond to aggregate tasks performed by the processes (e.g., read from a file).

An interesting and important observation is that since these hidden tasks should be the same, it should be possible to reliably correlate the simultaneous observable behaviors of the two processes when no attack is occurring, and to notice an increased behavioral distance when wormhole attack succeeds on one of them.

CONCLUSION AND FUTURE ENHANCEMENT

The client knows the data loss after it reached the intruder level. Client may trace back it but it is inefficient, because it takes more time to trace. The receiver checks the count of the packets and received packets if it is differed then they know that data may hacked. The existing system is less flexible, less secure and also less compatible. Monitoring stub will helps to improve the efficiency of the trace back mechanism. Behavioral distance used to find out the hacking of information before the data corrupted or updated by the intruder. The proposed detection scheme manages to avoid false alarms. It is used to find out the hacking of information before the data is hacked. The further extensions of our work may also facilitate fighting against wormhole attacks on encrypted protocols in the mobile ad hoc environment.

REFERENCES

[1] Garcia-Teodoro; J. Diaz-Verdejo; G. Macia-Fernandez; E. Vazquez., "Anomaly-based network intrusion detection: Techniques, systems and challenges(2009)", Computers& SecurityVolume 28, Issues 1–2, February–March 2009, Pages 18–28,Elsevier.

[2] Y. Hu, A. Perrig, and D. Johnson: "Packet leashes: a defense against wormhole attacks in Wireless Ad Hoc Networks". In Proceedings of the IEEE Conference on Computer Communications (Infocom), 2003.

[3] J. Zhen and S. Srinivas. "Preventing replay attacks for secure routing in ad hoc networks". Proc. of 2nd Ad Hoc Networks & Wireless (ADHOCNOW' 03), pp. 140--150, 2003.

[4] Hon Sun Chiu King-Shan Lui, "DelPHI: Wormhole Detection Mechanism for Ad Hoc Wireless Networks", International Symposium on Wireless Pervasive Computing ISWPC 2006.

[5] Levente Buttyán, László Dóra, István Vajda: "Statistical Wormhole Detection in Sensor Networks". Second European Workshop on Security and Privacy in Ad Hoc and Sensor Networks (ESAS 2005) Visegrád, Hungary, July 13-14, 2005: 128-141

[6] Lijun Qian, Ning Song, and Xiangfang Li. "Detecting and locating wormhole attacks in Wireless Ad Hoc Networks through statistical analysis of multi-path". IEEE Wireless Communications and Networking Conference - WCNC 2005.

[7] Phuong Van Tran; Le Xuan Hung; Young-Koo Lee; Sungyoung Lee; and Heejo Lee, "TTM: An Efficient Mechanism to Detect Wormhole Attacks in Wireless Ad-hoc Networks(2007)" Asia-Pacific Service Computing Conference, The 2nd IEEE,pp 172-178 on 11-14 december 2007.

[8] Shi Zhicai, Xia Y ongxiang, "A Novel Hidden Markov Model for Detecting Complicate Network Attacks" Wireless Communications, Networking and Information Security (WCNIS), 2010 IEEE International Conference on 25-27 june 2010.

[9] Subramanian Neelakantan , Shrisha Rao, “A Threat-Aware Anomaly-Based Intrusion-Detection Approach for Obtaining Network-Specific Useful Alarms” ICDCN 2009, LNCS 5408, pp. 175–180, 2009. @ Springer-Verlag Berlin Heidelberg 2009.

[10] Rutvij H. Jhaveri, Ashish D. Patel, Jatin D. Parmar, Bhavin I. Shah, “ MANET Routing Protocols and Wormhole Attack against AODV”, IJCSNS International Journal of Computer Science and Network Security, VOL.10 No.4, April 2010.

[11] V. Jyothsna, V. V. Rama Prasad, K. Munivara Prasad,“A Review of Anomaly based Intrusion Detection Systems”, International Journal of Computer Applications (0975 – 8887)
Volume 28– No.7, August 2011. [13] Zaw Tun, Aung Htein Maw, “Wormhole Attack Detection in Wireless Sensor Networks”, World Academy of Science, Engineering and Technology 46 2008.

[12] Zaw Tun and Aung Htein Maw, “Wormhole Attack Detection in Wireless Sensor Networks”, World Academy of Science, Engineering and Technology 46 2008.

[13] I. Khalil, S. Bagchi, and N.B. Shroff. “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”. In proceeding of International Conference on DependableSystems and Networks (DSN 2005), Yokohama, Japan.

[14] I. Khalil, S. Bagchi,N.B. Shroff., “LITEWORP: A Lightweight Countermeasure for the Wormhole Attack in Multihop Wireless Networks”. In proceeding of International Conference on DependableSystems and Networks (DSN 2005), Yokohama, Japan.

[15] Saurabh Gupta, Subrat Kar, S Dharmaraja,“WHOP: Wormhole Attack Detection Protocol using Hound Packet”, pp (226-231) Innovations in Information Technology (IIT) 2011.

[16] Ming-Yang Su. “Warp: A wormhole-avoidance routing protocol by anamoly detection in mobile ad hoc networks”,Computer Security, vol.29, March 2010.

[17] Sung-Bae Cho, Hyuk-Jang Park, “Efficient anomaly detection by modeling privilege flows using hidden Markov model,” Computers& Security, vo1.22, Jan. 2003, pp. 45-55.

[18] German Florez-Larrahondo, Susan M. Bridges, Rayford Vaughn, “Efficient modeling of discrete events for anomaly detection using hidden Markov models,” Proc. of the 8th International Conference on Information Security, Sep. 2005, pp. 506-514.

[19] Andr'e Ames, Fredrik Valeur, Giovanni Vigna, and Richard A. Kemmerer, “Using hidden Markov models to evaluate the risks of intrusions,”Proc. of the Recent Advances in Intrusion Detection (RAID 2006) Symp., Sep. 2006, pp. 1 45-164.

[20] Zhang Song-hong, Wang Ya-di, Han Ju-hong, “Approach to forecasting multi-step attack based on HMM,” Computer Engineering, vo1.34, pp (131 -133) March 2008.