Mohammad Alam Basha / International Journal of Engineering Research and Applications (IJERA) ISSN: 2248-9622 www.ijera.com
Vol. 2, Issue 3, May-Jun 2012, pp.2242-2247

A Simplified Approach To Agent Based Efficient Anomaly Intrusion Detection in Ad-Hoc Networks Using Honey Tokens.

Mohammad Alam Basha
Pursuing M.tech (cse) from K.B.N.C.E., Gulbarga.
Affiliated to VTU Belgaum, Karnataka.
Under the guidance of: Prof. Asma Parveen,
Asst. prof. K.B.N.C.E., Gulbarga.

Abstract:

Networks are protected using firewalls but when wireless networks are being used, the information in the network leaks like a sieve and information passes right over the firewall in both the directions. Hence these firewalls are not sufficient and effective in wireless networks. And even many intrusion detection systems are used in mobile ad-hoc networks like a).Signature-based IDS which is incapable of detecting novel threats and b). Anomaly detection scheme which can detect novel attacks but require much overhead , requires more processing capacity, and minor changes in the networks cannot be determined hence generate false positives. These IDS focus on either routing protocols or its efficiency, but it fails to address the security issues. Hence the ultimate goal of the security solutions for wireless networks is to provide security services, such as authentication, confidentiality, integrity, anonymity, and availability, to mobile users. This paper incorporates agents and data mining techniques to prevent anomaly intrusion in mobile adhoc networks. Home agents present in each system collects the data from its own system and using data mining techniques to observe the local anomalies. The Mobile agents monitoring neighboring nodes and collect the information from neighboring home agents to determine the correlation among the observed anomalous patterns before it will send the data. This system was able to stop all of successful attacks in an adhoc networks and reduce false alarm positives.

Keywords: Firewalls, Mobile agents, Intrusion Detection (IDS), Ad-hoc networks.

I. Introduction:

Intrusion detection is an important part of security related to computers. It is used to detect attacks and other security violations that are not prevented by other security mechanisms. A mobile ad-hoc network is basically the collection of wireless mobile hosts forming a dynamic networks infrastructure in absence of centralized monitoring system [26]. These are also called as MANETS. The mobility nature of MANTES leads to many issues, one of the biggest issues is the security in network due to lack of centralized monitoring system. It is very important to protect these kinds of networks. But the traditional way of protecting wired and wireless networks using firewalls has proven no longer sufficient to protect MANETS [7]. This is because of Potentially Unwanted Programs (PUPs): PUP is the collective term given to programs whose presence poses a serious security and privacy threat to users. This includes malware, spyware, adware and other myriad programs. The commercial incentives of these programs are lucrative enough for this 'industry' to thrive, and according to some projections, are expected to rise at exponential rates in the future. The success of any spyware on a system is determined by its ability to evade detection. Towards this goal, early spyware had the advantage of user ignorance and lack of security mechanisms or tools to detect and remove them. Since then, various anti-spyware mechanisms like toolbars, various detection and removal tools, etc., have been developed. These defense solutions employ either signature based or anomaly detection (flow based) philosophies. Even though signature based systems have the advantage of detecting known spyware programs with a high degree of accuracy, they are incapable of detecting novel threats. Anomaly detection schemes, on the other hand, are capable of detecting new threats with reasonable accuracy. They operate on the premise that any behavior observed in a system that deviates from the 'normal' behavior is indicative of the presence of unauthorized actions.

Given the history of spyware creation and operation, it is quite likely that the next update of spyware will attempt to bypass this mechanism too. The work in this paper presents a methodology whereby simple mechanisms like honey token generation can be detected by a new class of spyware called SpyZen.

II. Related Works:

Traditional security mechanism such as intrusion detection system, firewall and encryption methods are not sufficient to provide security in an adhoc networks. Countering threats to an organization's wireless adhoc network is an important area of research. Intrusion detection means identifying any set of actions that attempt to compromise the integrity, confidentiality or availability of resource [3]. Many techniques have been discussed to prevent attacks in an wireless adhoc networks as follows. Ricardo Puttini et al [16], propose design and development of the IDS are considered in 3 main stages. A parametrical mixture model is used for behavior modeling from reference data. The associated Bayesian classification

leads to the detection algorithm [15]. MIB variables are used to provide IDS needed information. Experiments of DoS and scanner attacks validating the model are presented as well. João B. D. Cabrera Et al [17], provides the solution of intrusion detection in Mobile Ad-Hoc Networks (MANETs), utilizing ensemble methods. A three-level hierarchical system for data collection, processing and transmission is described. Local IDS (intrusion detection systems) are attached to each node of the MANET, collecting raw data of network operation, and computing a local anomaly index measuring the mismatch between the current node operation and a baseline of normal operation. The complete suite of algorithms was implemented and tested, under two types of MANET routing protocols and two types of attacks against the routing infrastructure. Yongguang Zhang et al [18], propose new intrusion detection and response mechanisms are developing for wireless ad- hoc networks. The wireless ad-hoc network is particularly vulnerable due to its features of open medium, dynamic changing topology, cooperative algorithms, lack of centralized monitoring and management point, and lack of a clear line of defense. Many of the intrusion detection techniques developed on a fixed wired network are not applicable in this new environment. Farroq et al [19] propose the signature detection technique and investigate the ability of various routing protocols to facilitate intrusion detection when the attack signatures are completely known. We show that reactive ad-hoc routing protocols suffer from a serious problem due to which it might be difficult to detect intrusions even in the absence of mobility. Mobility makes the problem of detecting intruders harder.

Vijay Bhuse et al [10], propose lightweight methods to detect anomaly intrusions in wireless sensor networks (WSNs). The main idea is to reuse the already available system information that is generated at various layers of a network stack. This is the different approach for anomaly intrusion detection in WSNs. Hongmei Deng et al [21], proposes the underlying distributed and cooperative nature of wireless ad hoc networks and adds one more dimension of cooperation to the intrusion detection process. That is, the anomaly detection is performed in a cooperative way involving the participation of multiple mobile nodes. Unlike traditional signature-based misuse detection approaches, the proposed scheme detects various types of intrusions/attacks based on the model learned only from normal network behaviors. Without the requirements of pre-labeled attack data, the approach eliminates the time-consuming labeling process and the impacts of imbalanced dataset.

Bo Sun et al [22], propose we first introduce two different approaches, a Markov chain-based approach and a Hotelling's T2 test based approach, to construct local IDSs for MANETs. Then demonstrate that nodes' moving speed, a commonly used parameter in tuning IDS performances, is not an effective metric to tune IDS performances under different mobility models. To solve this problem, author further propose an adaptive scheme, in which suitable normal profiles and corresponding proper thresholds can be selected adaptively by each local IDS through periodically measuring its local link change rate, a proposed unified performance metric.

Haiguang Chen et al [23], propose lightweight anomaly intrusions detection. In the scheme, author investigates different key features for WSNs and defines some rules to building an efficient, accurate and effective Intrusion Detection Systems (IDSs). We also propose a moving window function method to gather the current activity data. The scheme fits the demands and restrictions of WSNs. The scheme does not need any cooperation among monitor nodes. Simulation results show that the proposed IDSs are efficient and accurate in detecting different kinds of attacks.

Gabriela F. Cretu et al [24], propose the use of model exchange as a device moves between different networks as a means to minimize computation and traffic utilization. Any node should be able to obtain peers' model(s) and evaluate it against its own model of "normal" behavior.

Yu Liu et al [25], propose game theoretic framework to analyze the interactions between pairs of attacking/defending nodes using a Bayesian formulation. We study the achievable Nash equilibrium for the attacker/defender game in both static and dynamic scenarios. The dynamic Bayesian game is a more realistic model, since it allows the defender to consistently update his belief on his opponent's maliciousness as the game evolves. A new Bayesian hybrid detection approach is suggested for the defender, in which a lightweight monitoring system is used to estimate his opponent's actions, and a heavyweight monitoring system acts as a last resort of defense.

Many authors proposed different techniques to prevent attacks in wireless adhoc networks. they mainly focused on signature based system, Anomaly detection scheme and creating static honey tokens to detect the anti-spyware. The signature based approach signature based systems have the advantage of detecting known spyware programs with a high degree of accuracy; they are incapable of detecting novel threats

The Anomaly detection scheme is used to monitor the system whether there is any deviation in the process. It observed in a system that deviates from the 'normal' behavior is indicative of the presence of unauthorized actions. The new class of spy ware overcomes these processes by hacking with the user process without any deviation in the system[26].

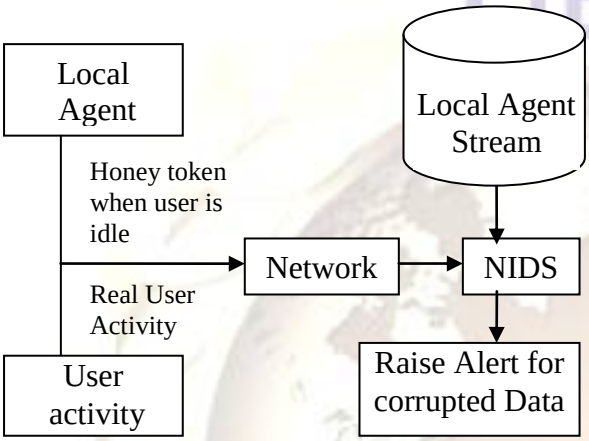
III. Our Approach

This paper incorporates new methodology such as mining and agents to provide solutions against wireless networks[26].Our Proposal incorporates that, given the history of spyware creation and operation; it is quite likely that the next update of spyware will attempt to bypass this mechanism too. The work in this paper presents a methodology whereby simple mechanisms like honey token generation can be detected by a new class of spyware called SpyZen. The basic concept behind our scheme is quite intuitive. SpyZen spyware operates in three stages.

The first stage is an 'install and observe' stage, where spyware merely listens to the sequence of events, of which certain portions are honey tokens.

In the second stage of analysis and inference, spyware detects the honey token sequence. Using data analysis algorithms like Associative Rule Mining algorithm, spyware can infer the honey token generation.

The third stage is the actual operation stage, where spyware operates only when the honey token sequence is not detected. We then present a defense mechanism against this new class of spyware, called SpyCon, which utilizes a randomized honey token generation scheme.



Dataflow Diagram

Modules used in this work are as follows:

a. Host agent:

This is at the client side. Host connects to the server through the proper port , once the connection is set then the, Host request for a page, request is sent to the server through the Spycon. If there is no syware detected by the spycon then the requested is served by the server.

b. Creating SpyZen

In this module, spyware named as SpyZen is created. This SpyZen avoids detection from the existing systems like Signature based detection systems, Anomaly based detection systems. SpyZen can also avoid detection from static honey token detection systems.

c. Generating randomized honey token

In this module, randomized honey token are generated. This randomized honey token is used to detect our spyware named as SpyZen. Honey tokens are generated in a random manner to help the SpyCon to detect our new kind of spyware.

d. Creating SpyCon

In this module we design the anti spyware called SpyCon. SpyCon is used to detect the new class of spyware called as SpyZen. SpyCon detects the SpyZen with the use of randomized honey token generation technique.

IV. Experimental Results

1. To illustrate the disadvantage of Signature based IDS:

Our project is designed so that it illustrate the disadvantages of traditional intrusion detection schemes like Signature based and Anomaly based Intrusion Detection.

In Signature-based IDS approach- Intrusion is determined using the Static Honey Token hence novel spyware are no detected.

As said earlier our project aims at designing new Spyware called as Spyzen which is capable of defeating current state of art of anti-spyware techniques. As this is a novel Spyware it is obvious that it will not be detected by Signature-based ids, hence host agent still assumes that no one is hacking the information but the hacker is on the other hand is easily reading the sensitive data.

2.Working of Spycon(A new approach to detect new spyware-i.e., Spyzen in our project)

Spycon is the anti-spyware which is used to detect new class of spyware called Spyzen. This spycon unlike signature-based IDS which uses static honey tokens to determine spyware, spycon uses randomized honey token generation technique to determine novel spywares.

Once the spyware is determined by the spycon, it is viewed by host agent easily. As soon as the host encounters Spyzen, host shut downs itself and restart itself once again by the time anti-spyware (spycon) removes the spyware (Spyzen). Now host can easily communicate the server this time intruder will not be able to view anymore information.

Figure 1:Static Honey Token is selected in host and requests for a page from server.

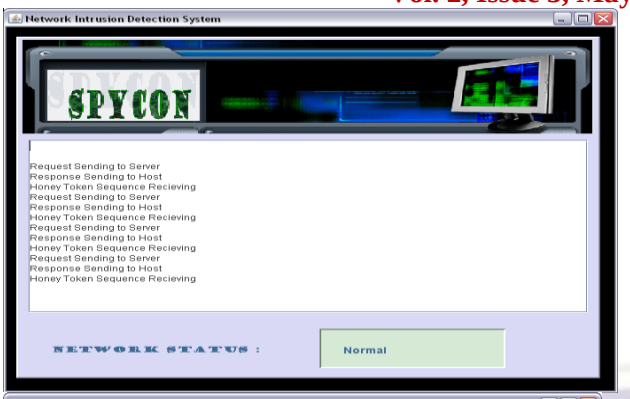


Figure 2: As Static honey token selected, new Spyware bypass anti-syware. Hence network status is still normal though the honey tokens are receiving.

Figure 3: but as we are using the Spycon, which is acts as anti-spyware detects the spyware

Figure 4: Advanced syware , SpyZen is detected.

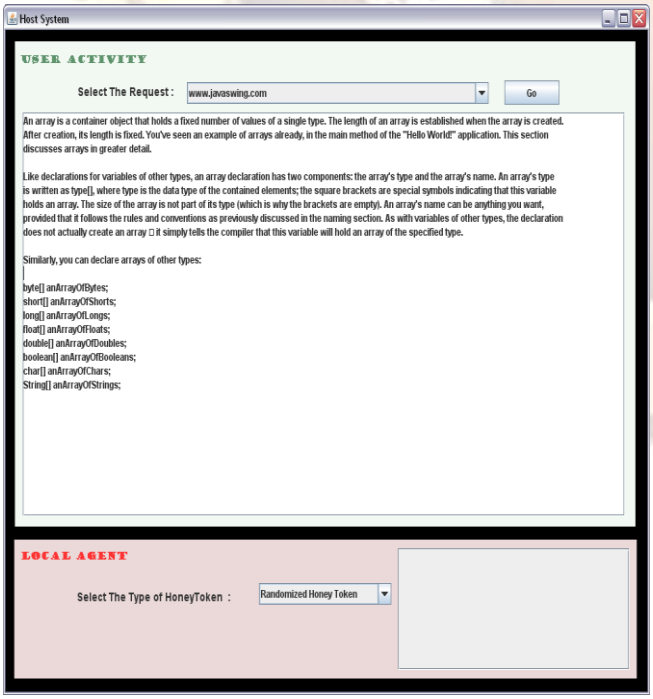


Figure 5:Randomized honey token is selected from host.

Figure 6: This time as Randomizes honey token is selected, advanced Spyware is detected.

V. Conclusion

In this project, we presented a new class of spyware called SpyZen that is capable of defeating current state of- the-art anti-spyware techniques. SpyZen operates in a surreptitious manner by blending in with legitimate user activity. It also defeats anti-spyware schemes that generate deterministic honey tokens to trick spyware into assuming legitimate user activity. To counter spyware like SpyZen, we devised a randomized honey token generation scheme called Spy- Con that addresses the inherent disadvantages of static honey token generation.

Hence, Traditional security mechanism such as IDS and firewall have not been sufficient to provide the security of wireless networks, however, this mechanism is able to block abnormal approach to wireless networks and to detect previously unknown attacks as well as variations of known attacks. Lastly it is concluded that our project overcomes the problem of false negative.

VI. References

[1] Y. Zhang and W. Lee, 'Intrusion Detection in Wireless AdHoc Networks', 6th Int'l. Conf. Mobile Comp. and Net. Aug.2000, pp. 275-83.

[2] Y. Zhang, W. Lee, and Y. A. Huang, 'Intrusion Detection Techniques for Mobile Wireless Networks', ACM J. Wireless Net., vol. 9, no. 5, Sept. 2003, pp.545-56.

[3] Amitabh Mishra, Ketan Nadkarni, and Animesh Patcha,Virginia Tech 'Intrusion Detection in Wireless Ad Hoc Networks', IEEE Wireless Communications, February 2004,pp. 48-60.

[4] Y. Huang, W. Fan, W. Lee, and P. S. Yu, 'Cross-Feature Analysis for Detecting Ad-Hoc Routing Anomalies',Proceedings of the 23rd IEEE International Conference on Distributed Computing Systems, 2003, pp. 478-487.

[5] Yu Liu, Yang Li and Hong Man, 'MAC Layer Anomaly Detection in Ad Hoc Networks', Proceedings of the 6th IEEE Information Assurance Workshop, June 17, 2005, pp. 402-409.

[6] B. Sun, K. Wu, and U. Pooch, 'Routing Anomaly Detection in Mobile Ad Hoc Networks', Proceedings of the 12th IEEE Int'lConf. on Computer Communications and Networks (ICCCN'03), Dallas, TX, Oct. 2003, pp. 25-3 1.

[7] Rena Hixon, Don M. Gruenbacher, 'Markov Chains in Network Intrusion Detection', Proceedings of the IEEE Workshop on Information Assurance, United States Military Academy, 2004, pp.432-433.

[8] Yia-an Huang, Wenke Lee, 'A Cooperative Intrusion Detection System for Ad hoc Networks', Proceedings of the Ist ACM Workshop on Security of Ad hoc and Sensor Networks, 2003, pp. 135-147.

[9] S. Jha, K. Tan, and R. Maxion, 'Markov chains, classifiers, and intrusion detection', Proceedings of 14th IEEE Computer Security Foundations Workshop, 2001, pp. 206-219

[10] Baolin Sun, Hua Chen, Layuan Li, 'An Intrusion Detection System for AODV', Proceedings of the 1 oth IEEE International Conference on Engineering of Complex Computer Systems (ICECCS '05), 2005, pp. 358-365.

[11] Iaonna Stamouli, Patroklos G. rgyroudis, Hitesh Tewari,'Real-time Intrusion Detection for Ad Hoc Networks', Proceedings of the 6th IEEE International Symposium on a World of Wireless Mobile and Multimedia Networks, 2005,pp. 374-380.

[12] A.A.Cardenas, S.Radosavac, J.S.Baras, 'Detection and Prevention of MAC Layer Misbehavior in Ad Hoc Networks', Proceedings of the 2nd ACM workshop on Security of Ad hoc Networks and Sensor Networks, 2004, pp. 17-22.

[13] Daniel C.Nash, Thomas L. Martin, Dong S. Ha, and MichaelS. Hsiao, 'Towards an Intrusion Detection System for BatteryExhaustion Attacks on Mobile Computing Devices' IEEE Int'l Conf. on Pervasive Computing and Communications Workshops, 2005, pp. 141-145.

[14] T.Martin, M.Hsiao, D.Ha, and J.Krishnaswami, 'Denial of Service Attacks on Battery-powered Mobile Computers',Second IEEE International Conference on Pervasive Computing and Communications, March 2004, pp. 309-318.

[15] Hang Yu Yang, Li-Xia Xie, 'Agent based Intrusion Detection for a Wireless Local Area Network', Proceedings of the IEEE third International Conference on Machine Learning and Cybermatics, 2004, pp. 2640-2643.

[16] Ricardo Puttini, Maíra Hanashiro, Javier García-Villalba, C. J. Barenco, " On the Anomaly Intrusion-Detection in Mobile Ad Hoc Network Environments", Personal Wireless Communications ,Volume 4217/2006, Springer link, September 30, 2006

[17] João B. D. Cabrera, Carlos Gutiérrez , Raman . Mehra ,"Ensemble methods for anomaly detection and distributed intrusion detection in Mobile Ad-Hoc Networks", Volume 9 , Issue 1 (January 2008) table of contents, Pages 96-119 , Elsevier Science Publishers, 2008.

[18] Yongguang Zhang , Wenke Lee, " Intrusion detection in wireless ad-hoc networks", Pages: 275 - 283 Year of Publication: 2000 ISBN:1-58113-197-6, ACM, 2000.

[19] Farooq Anjum Dhanant Subhadrabandhu and Saswati Sarkar,"Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A comparative study of various routing protocols", Seas, 2008.

[20] Vijay Bhuse , Ajay Gupta , " Anomaly intrusion detection in wireless sensor networks" , Special issue on trusted internet workshop (TIW) 2004, Journal of High Speed Networks, Volume 15 , Issue 1 (January 2006), ACM, 2006.

[21] Hongmei Deng; Xu, R.; Li, J.; Zhang, F.; Levy, R.; Wenke Lee, " Agent-based cooperative anomaly detection for wireless ad hoc networks", Parallel and Distributed Systems, Volume 1, Issue , 0-0 0 Page(s):8, 2008.

[22] Bo Sun 1 *, Kui Wu 2, Yang Xiao 3, Ruhai Wang 4, "Integration of mobility and intrusion detection for wireless ad hoc networks", 2006.
[23] Haiguang Chen, Peng Han, Xi Zhou, Chuanshan Gao, "Lightweight Anomaly Intrusion Detection in Wireless Sensor Networks", Intelligence and Security Informatics, Springer link, 2007.
[24] Gabriela F. Cretu, Janak J. Parekh, Ke Wang, Salvatore J. Stolfo, "Intrusion and Anomaly Detection Model Exchange for Mobile Ad-Hoc Networks.
[25] Yu Liu, Cristina Comaniciu, Hong Man, "A Bayesian Game Approach for Intrusion Detection in Wireless Ad Hoc Networks", ACM 159593507X, 2006.
[26] R. Nakkeeran, T. Aruldoss Albert and R.Ezumalai "Agent Based Efficient Anomaly Intrusion Detection System in Adhoc network" IACSIT International Journal of Engineering and Technology Vol. 2, No.1, February, 2010.

Author,s Profile:

Mr.Mohammad Alam Basha pursuing M. Tech in Computer Science and Engineering from K. B. N. College of Engineering Gulbarga. Affiliated to V. T. U., Belguam, Karnataka. Presently working with Govt. Polytechnic, Raichur as Lecturer in the Department of Computer Science and Engineering.