International Journal of Engineering Research and General Science Volume 3, Issue 2, Part 2, March-April, 2015
ISSN 2091-2730

Detecting Malicious Traffic in Wireless Mesh Network

1 Ankur Rajput, 2 Sachin Goyal, 3Ratish Agrawal
1Cyber law& Information Security, NLIU, Bhopal, Madhya Pradesh, India
2, 3 Information Technology, RGPV, Bhopal, Madhya Pradesh, India

ABSTRACT- Wireless Mesh networks are intelligent work of electronics rely on wireless medium to communicate cheaper, dwindle and in cost efficient way which gained the interest of many of organizations. But the implementation of wireless nodes is always a matter of concern as they are vulnerable to many attacks. Creating Malicious nodes are favorite target of attackers. In recent years; malware has proliferated into wireless networks as these networks have grown in vogue and pervasiveness. Researcher in this report propose a inbuilt framework for every mesh network like a honey pot specially designed for crafted packets which initially detect suspicious behavior, and suspicious entries regarding a particular node reaches a set threshold, that node is declared ambiguous then all the traffic at that node will be again send for root kit analysis at the virtual environment which was created inside that honey pot to detect zero days exploits and reduce the false positives.

Keywords: Cross Word Mesh Network (CMN), Dominant Attacks, Malicious Nodes, crafted packets, Honey pots, Bot Minor Detection, Intrusion Detection System (IDS).

I. INTRODUCTION

Malwares poses a corporeal threat to the wireless computing infrastructure which is not fixed even as nodes are mobile these days due to mesh environment and there is no root node to control, each and every node know details about neighbor for communication, so attackers launch attacks on every nodes that vary from the less nosy confidentiality or privacy attacks, such as traffic analysis & eavesdropping, to the more nosy methods that disrupt the nodes normal functions to get privileges mostly are malware attacks and even alter the network traffic to destroy the integrity of the information, such as unauthorized access and session hijacking attacks [1], [2].The boom of wireless network in organization on one hand and on the other side unauthorized attackers spreading malware and creating hosts as Bots for various different attacks has motivated to design effective security mechanism for detecting malicious traffic at mesh network.

Researcher planned for creating an integrated countermeasure to prevent from zero days hazards before the attackers compromise the single node. Dominant attacks on these networks such as the worm hole [3], sinkhole [4], and Sybil [5], that bestow vulnerabilities in the routing protocols are researched a lot and their best defense mechanism, have been investigated before they were actually launched by the researcher .Momentous research has been done in detecting intrusion in ad hoc networks and most of researchers faced the problem of detecting malicious node in wireless sensor network facing huge number of false positives. Three well known research papers on detecting malicious nodes in sensor networks are "Mitigating Routing misbehavior by Marti et al." [6], Towards Intrusion Detection in WSN by Loanis and Dimitriou [7], and Suspicious Node Detection by Signal Strength by Junior et al. [8]. Different approaches are followed by each researcher, Signal strength was used to detect malicious node in [8], where message transmission is considered suspicious if strength is incompatible with geographical position was adequately effective as in result, else other were poorer as estimated by researchers. Xiao et al. developed a mechanism for rating sensors in terms of correlation by exploring Markov Chain [9].Atakli et al. [10] presented a malicious node detection scheme using weighted trust evaluation for three-layer hierarchical network architecture. Core values are selected to identify malicious nodes behaving opposite to the sensor readings which are amended depending on the distribution of acquaint ant nodes. Another Remolded detection scheme based on weighted trust evaluation

was proposed in [11]. Amending the core values at each node was the new scheme used, few of management schemes have been proposed in routing and communications [12]. Some efforts are also being made to combine communication and data trusts [13]. But malware coders still compromised these nodes as graph shown by 2014 annual security reports of Cisco [14], Semantics [15] & McAfee [16].

In this paper researcher as preliminary proposed an Associate-based malicious node detection scheme for wireless mesh networks taken light from "Neighbor-Based Malicious Node Detection in Wireless Sensor Networks"& "Malicious Node Detection Using Confidence Level Evaluation" in a Grid-Based Wireless Sensor Network by Sung-Jib Yim, Yoon-Hwa Choi which identifies nodes to be malicious if they don't behave similar to normal nodes and then for identifying Botnet and root kits used Bot minor Architecture framework on suspicious nodes[17].Researcher of this paper was influenced by node detection mechanism considering grid based network achieving Confidence levels and weighted majority voting are employed to detect and isolate malicious nodes, without sacrificing normal nodes and degrading event detection accuracy [18] [19].

A more recent report from McAfee says "malware continues to grow" [20]. Thousands of new malware appear very quickly, reports from G Data and King soft Laboratory said. Many security researchers are using different mechanism to detect malicious nodes but are lacking as malwares are becoming smarter every day and polymorphic malware are the newcomer in this destructive game of defeating the opponent as they are capable of self-reproduction, and adopts different identity from its parent nodes. Root kits are the major concern as they were hidden and packed inside the processes make them much harder to detect. So here in this report after analyzing the suspected node all the inbound and outbound traffic passing through that node passed through the virtual machine presented inside the honey pot and further analysis would be done following the process level approach to detect all the Zero Day attack and reduce false positives.

PRELIMINARY

The preparation of Detection of malicious node and then analyzing root kit via honey pot needs a Network model in which we can perform both the scenarios for identifying malware.

CROSS WORD MESH NETWORK

A Cross-word Puzzle shape mesh network is assumed divided into four square shaped grids A through D and L is the length of sides as illustrated in figure 1

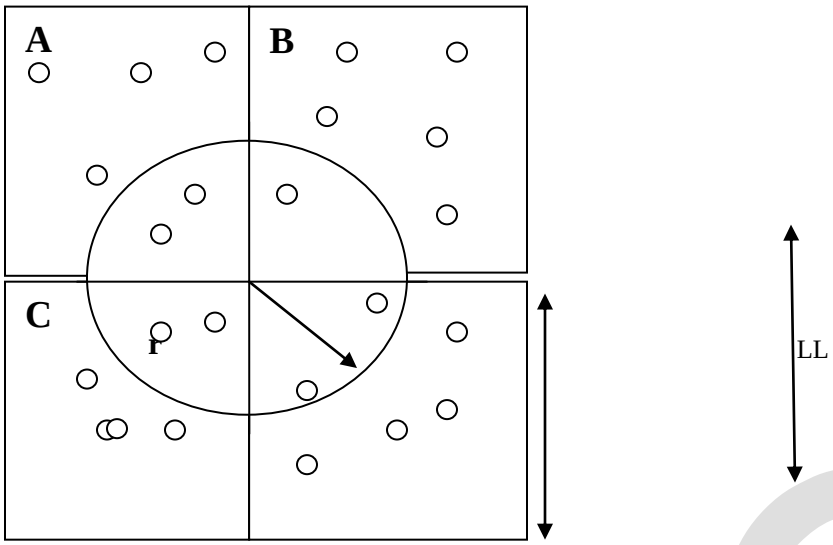


Figure 1: Mesh Network with 4 grids

Each Mesh node is assumed to know its own location, immediately after implementation the network carries out grid construction process, and each node figures out the grid in which they belongs. Mesh nodes in each grid form a cluster, where a cluster head is selected dynamically and all the other nodes in the cluster communicate directly with the cluster head. Two types of communication are defined here for malicious node detection: one for communication between the cluster head and cluster members and the other for communication between neighboring cluster heads.

Now come in picture the threshold test say majority voting, but the decision made by cluster heads might not be accurate for small event regions due to insufficient number of event nodes at each grid and lowering the threshold might be needed to achieve high event detection performance, causing a considerably high false alarm rate, unless the number of malicious nodes is negligibly small. So we will consider inter grid communication by finding the center of the nodes re- porting an alarm, and then apply a threshold test to the estimated event region.

PRE MODEL FOR FAULT DETECTION

In order to detect malicious nodes, Researcher defines a model for the nodes behavior assuming that all the nodes become malicious randomly and independently with the same probability P_m and it is assumed that each malicious node sends its report inconsistent with the actual sensor reading with the probability P_{ma} which means that malicious node will report 1(0) with the probability Pma when actual reading is 0(1). In appendage normal sensor nodes are also assumed to report against their readings, randomly and independently, with the same probability P_t. Hence malicious nodes must be detected and isolated in the presence of such faults and events.

FALSE ALARM DETECTION

Identifying malicious nodes can create plenty of false alarms thus detecting them would be the major task in an event region. Figure 1 defines the event region which is used throughout the detection process assumed to be a circle with radius r, although the proposed scheme can be applied to event regions of other shapes with minor modifications. Now selecting threshold value for event detection to be malicious, the size of region plays an important role. In our case size of grid is L and radius is r so average number of node will be

$$N_a = d.\ \pi r^2/L^2$$

Where d is the average number of sensor nodes, now comes the vital task to set the threshold value of nodes for detection and theoretically it is easy to set the threshold for large event region as compare to small event region because on small event nodes when region lies across multiple adjacent grids and in that case choosing proper threshold might be difficult or sometimes impossible to satisfy both high event detection accuracy and low false alarm rate.

NODE DETECTION MECHANISM

Monitoring Mechanism

Dynamic and scalable nature of mesh node is the key term used here to detect the malicious node by observing the behavior of neighbor nodes, for example message sending node A observes the packet receiving node B functioning and converts itself to monitoring node and audit the behavior of node B when it send packets to other neighbor nodes to check whether it alters the packet contents other than adding its header information. If there is a difference between the original and actual messages greater than a certain threshold, the message is considered suspicious and updated in the table that Node B is now considered suspicious. Each node builds a Suspicious Node table containing the reputation of nodes in the cluster and table contains the node ID, the number of suspicious and unsuspicious entries. Nodes update this table every time they identify suspicious activity.

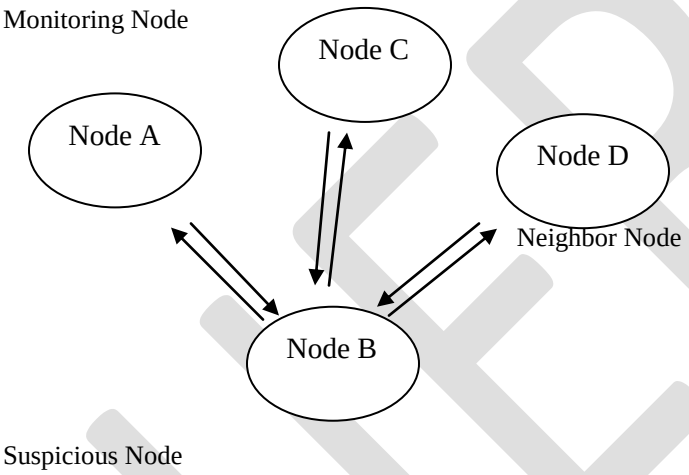


Figure 2: Suspicious Node Detection

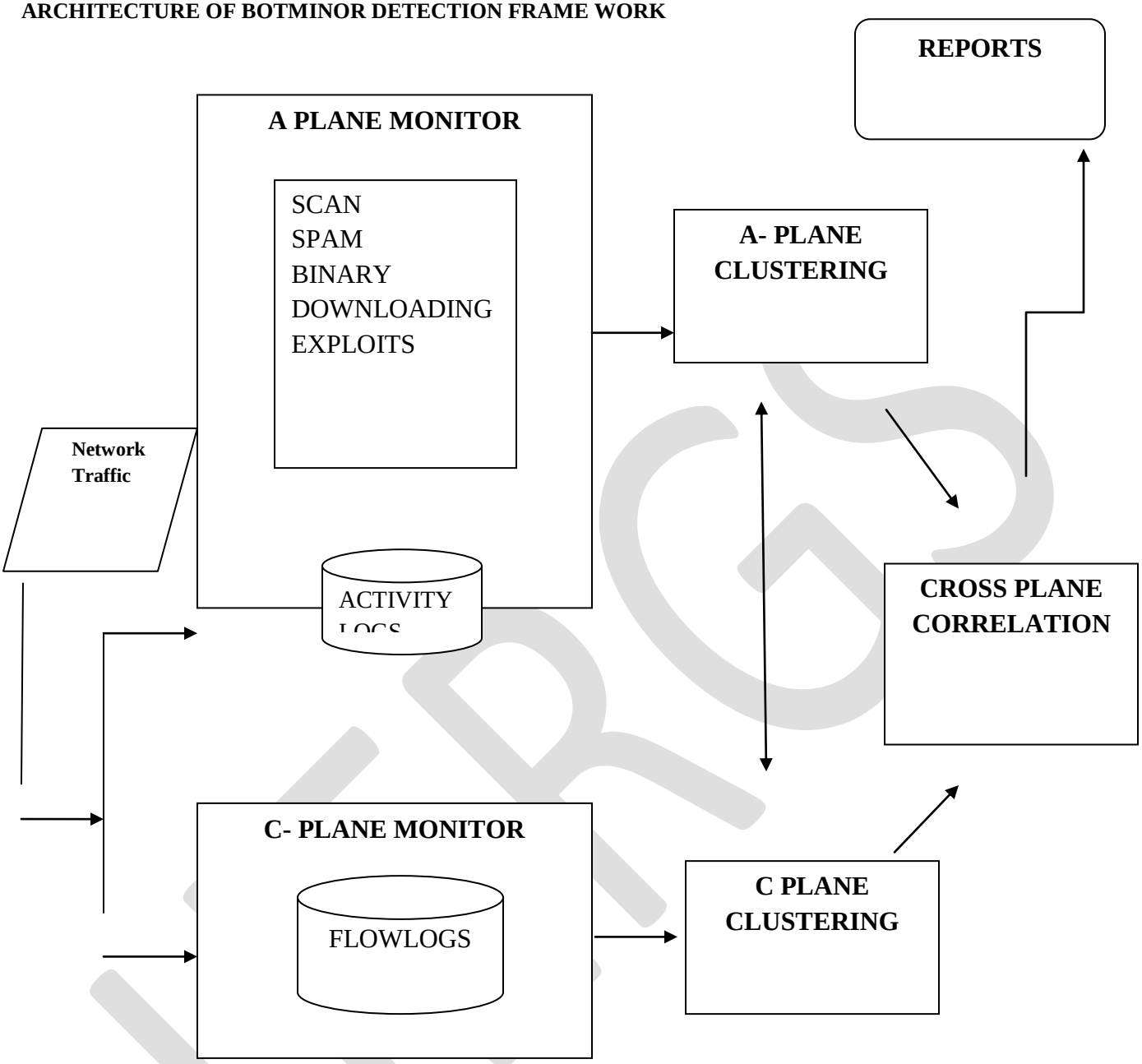
A malicious node is a compromised node in which attacker has somehow managed to break the encryption and has gained access to the secure keys and routing protocols of the Mesh network. After analyzing the behaviors.

monitoring node get the details of compromised credentials and this proposed model could be a countermeasure for these attacks.

BOT MINOR DETECTION

Bots are autonomous program performing the tasks which are more recent trend in malicious development. As we had detected suspicious node by behavior analysis but when it comes to root kits many times they bypass the strings signatures, behavior patterns very easily by hiding the process in linker and causes harm like zero days exploits. In order to avoid the botnet attack researcher presented botminer detection framework architecture which monitors the network traffic of suspicious node and perform two phase monitoring and clustering then analyze the cross plane correlation and generates the report which is so effective as activity logs and flow logs are compared and clustering process detect the hidden malwares.

ARCHITECTURE OF BOTMINOR DETECTION FRAME WORK



It was proposed to monitor communication and actions of suspicious nodes in specified events to check whether there were any kind of overlapping between two sets. For Example If two nodes behaves similarly in communicating with some other entity or in performing action then there is chances that they must belongs to a specific botnet. Monitoring would be the first phase and traffic is sent to different monitoring systems A-PLANE Monitor and C-PLANE Monitor.

MONITORING SYSTEM

C-PLANE MONITOR

C-plane monitor captures network flows and record information on who is talking to whom. Network flows you can just imagine out of all the packets you observe raw network packets on the network, you just summarize this communication in flows so basically you have IP address of source, IP address of destination, source port, source destination and some information about what happens in the

flow for example number of bytes exchanged, time duration of exchanged packets exchanged per flow and stuff like that to understand exactly flow representation. Payload information is not considered at this level.

A-PLANE MONITOR

A-plane monitor log information on who is doing what and basically analyzes outbound traffic through the monitored traffic and tries to detect several malicious activities that internal node might perform. System tries to observe whether a node is starting a scan activity or its sending large quantity of spams basically to check Denial of service attack.

CLUSTERING SYSTEM

Now once we have the information of C-plane Monitor we just group together similar communications to group nodes communicating in similar manner. To speed up this process system performs basic filtering and white listing to eliminate internal to internal communication within a network which is already checked via node detection mechanism and white listing to eliminate destinations that are frequently contacted by hosts in general as common as famous website like Google and Yahoo etc.

Same mechanism is followed with A-plane data we get the list of clients performing malicious activity then initial cluster is performed on their activity for example grouping together nodes which are performing scanning then other group of host sending spams and nodes that try to perform DDOS, Binary Downloading etc. All on their own class and then we look for another type of clustering within each cluster for instance if you perform scan, we'll look towards what destination or towards which port then system creates different clusters. Idea is basically you have clusters of communications and clusters of activities you want to see whether you have overlapping hosts to check whether one host appears in many cluster which is done in cross plane correlation basic approach is to cross check clusters in the two plans for finding interesting intersection basically and at the end each node has given a score and based on this score if it's above the threshold then you will flag the host is been infected with the particular bot. The approach overall is quite effective with very low false positive rate and it's a good step forward to detect bot infection at network level.

CONCLUSION & FUTURE WORK

The malicious node detection mechanism with Bot minor framework prevents many routing attacks on mesh environment such as Wormholes, Sinkholes, Sybil attacks, Distributed Denial of Service and Botnet attacks. The criteria to detect maliciousness of node are also compared with set threshold which help in achieving less false positive rates and many organization are just performing single node mechanism which may lead to zero day attacks. Hence to avoid that they must consider defense in depth approach by following both the method to achieve security.

The major problems I faced while the detection is that approach rely on noisy behavior as observing communication and activity traffic. All the listed activity which we focused are noisy in general for example scanning looking for open ports, in denial of service sending large amount of data or sending unsolicited emails. But in practical scenario things are quite different attackers try to compromise silently on that account in future I will be using the same approach but add the another correlation approach at network level.

REFERENCES:

1. D. Welch and S. Lathrop, "Wireless security threat taxonomy," in Information Assurance Workshop, 2003. IEEE Systems, Man and Cybernetics Society, pp. 76–83, 2003
2. A. Herzog, N. Shahmehri, and C. Duma, "An ontology of information security," International Journal of Information Security and Privacy, vol. 1, no. 4, pp. 1–23, 2007.
3. Y. Hu, A. Perrig, and D. Johnson, "Packet leashes: a defense against wormhole attacks in wireless networks," in IEEE INFOCOM 2003.Twenty-Second Annual Joint Conference of the IEEE Computer and Communications Societies, vol. 3.
4. C. Karlof and D. Wagner, "Secure routing in wireless sensor networks: Attacks and countermeasures," Ad Hoc Networks, vol. 1, no. 2-3,pp. 293–315, 2003.
5. J. Douceur, "The Sybil attack," in Peer-to-Peer Systems, First International Workshop, IPTPS 2002, Cambridge, MA, USA, March 7-8, 2002,Revised Papers, pp. 251–260.
6. Marti, S., T. J., Lai, K. and Baker, M. "Mitigating routing misbehavior in mobile ad hocnet works". In Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (MobiCom 2000) August 6-11, 2000, Boston, USA. Boston, MA, ACM Press,pp. 255-265.
7. Loanis, K. and Dimitrou, T. "Towards intrusion detection in wireless sensor networks". In Proceedings of the 13th European Wireless Conference, April 1-4, 2007, Paris, France.
8. Junior, W., Figueiredo, T. and Wong, H. "Malicious node detection in wireless sensor net works". In Proceedings of the 18th International Parallel and Distributed Processing Symposium (IPDPS'04), April 26-30, 2004, Santa Fe, New Mexico
9. X.-Y. Xiao, W.-C. Peng, C.-C. Hung and W.-C. Lee, "Using Sensor Ranks for In-Network Detection of Faulty Readings in Wireless Sensor Networks, "International Workshop Data Engineering for Wireless and Mobile Access, Beijing, 10 June 2007, pp. 1-8.
10. I. M. Atakli, H. Hu, Y. Chen, W.-S. Ku and Z. Su, "Malicious Node Detection in Wireless Sensor Networks Using Weighted Trust Evaluation," Proceedings of Spring Simulation Multi-Conference, Ottawa, 14-17 April 2008, pp. 836-843.
11. L. Ju, H. Li, Y. Liu, W. Xue, K. Li and Z. Chi, "An Improved Detection Scheme Based on Weighted Trust Evaluation for Wireless Sensor Networks, "Proceedings of the 5th International Conference on Ubiquitous Information Technology and Applications, Sanya, 16-18 December 2010, pp. 1-6.
12. M. Momani and S. Challa, "Survey of Trust Models in Different Network Domain," International Journal Ad Hoc, Sensor & Ubiquitous Computing, Vol. 1, No. 3, 2010, pp. 1-19.
13. M. Momani, S. Challa and R. Alhmouz, "Can We Trust Trusted Nodes in Wireless Sensor Networks?" International Conference Computer and Communication Engineering, Kuala Lumpur, 13-15 May 2008, pp. 1227-1232.
14. http://www.cisco.com/web/offers/ip/2014-annual-security-report/
15. http://www.semantic.com/security_response/publications/threatreport.jsp
16. http://www.mcafee.com/in/resources/reports/rp-quaterly-threat-q4-2013.pdf
17. BotMiner: Clustering Analysis of Network Traffic for Protocol- and Structure-Independent Botnet Detection Guofei Gu, Roberto Perdisci, Junjie Zhang, and Wenke Lee.
18. Neighbor-Based Malicious Node Detection in Wireless Sensor Networks by Sung-Jib Yim, Yoon-Hwa Choi Department of Computer Engineering, Hongik University, Seoul, Korea Wireless Sensor Network, 2012, 4, 219-225

19. Malicious Node Detection Using Confidence Level Evaluation in a Grid-Based Wireless Sensor Network Min-Cheol Shin, Yoon-Hwa Choi Department of Computer Engineering, Hongik University, Seoul, Korea Wireless sensor Network 2013,5, 52-60
20. Mcafee and Lab, 2014 Threats Predictions. 2014

IJERGS