An Agent based Intrusion Detection System Architecture for Mobile Ad Hoc Networks using Ant Colony Algorithm

S. Sampath
Research Scholar,
Department of Computer Science,
Karpagam University,
Coimbatore, Tamilnadu, India.

V. Thiagarasu
Associate Professor,
Department of Computer Science,
Gobi Arts & Science College,
Gobichettipalayam, Tamilnadu, India

***Abstract*— There is a major security threat for Mobile Ad Hoc Networks (MANETs) because of its de-centralized dynamic nature The dynamic nature of MANETs forces a set of challenges to its effective implementation such as intrusion detection procedures which provides secured performance in MANET applications. In this paper, an agent based intrusion detection and prevention system has been designed using ant colony algorithm. Each node is monitored using a mobile agent of the MANET and each node runs a specific application. Multi-depot packet routing (MDPR) in Ant colony optimization is used to analyze the packets from multiple nodes join in MANET. Support vector machines (SVM) is used to identify the malicious activities of current packet with pre-recorded activities.**

Keywords*— Ad Hoc Network, MANET, IDS, MDPR, Mobile Agent

I. INTRODUCTION

A MANET is a type of ad hoc network that has no fixed infrastructure, can change locations and configure itself on the fly. Security is one of the major challenge to the applications on a MANET. An Intrusion Detection System (IDS) is a process of detecting and isolating to malicious activity located at computing and networking devices. A number of Intrusion Detection System architectures have been already developed. In this paper, an agent based IDS architecture using ant colony optimization for MANET has been introduced. This architecture, each node in the network implements a small piece of software called Mobile Agent that cares IDS detection and associated activities till the MANET vanish. Section 2 of this study compares with almost all existing techniques. The architecture has been implemented with the network simulator tool NS-2 and can also be implemented with Qualnet or Snort. Section 3 of this paper deals with the proposed detection technique. Section 4 explains the concept in Simulated environment. Results and findings are presented in Section 5. Section 6 Concludes.

II. RELATED WORK

Intrusion detection systems are implemented using software agents named mobile agents which is capable to flow from one node to another. These agents are used to identify any attacks from malicious nodes. There are different types of attacks[13] as below:

A. Passive Attacks: Without affecting the routing protocols the information about the node and network is collected. Two types of passive attacks[13] are 1. Eavesdropping: The wireless messages are inter-received without the knowledge of sender or receiver. Cryptographic messages can be used to safeguard from this type of attacks. 2. Traffic Analysis: Based on heave communications to important hosts, it is easily identified the importance of the specific host than others and hence targeted.

B. Active Attacks: There are four types of active attacks[7] i) Sleep Deprivation: One computing or network device communicates with another node and the attacker keeps the resources busy. ii) Black Hole: In this case, a malicious host in the middle drops malwares instead of packet transmission. iii) Grey Hole: The malwares are dropped to particularly selected host. iv) Sybil: with alternate congruence the attacker may forward packets may produce mayhem to block or disturb routing.

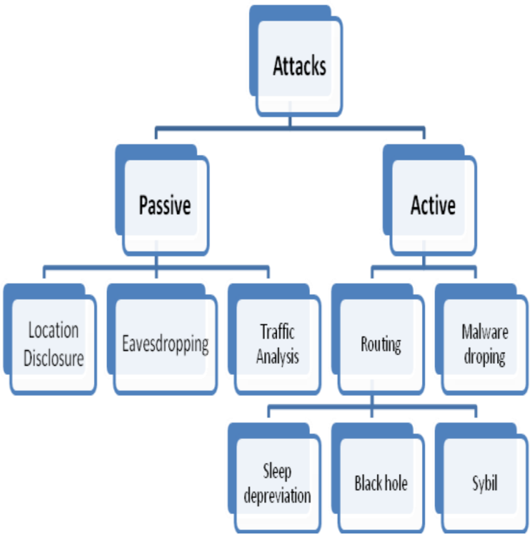


Fig.1: Types of attacks in MANET

III. PROPOSED IDS ARCHITECTURE

The proposed architecture is depicted in **Fig. 2**. Through self-organized collaboration these ID agents form a distributed intrusion detection system (DIDS). The sensor layer of an ID agent provides the interface to the network and the host on which the agent resides. Sensors acquire raw data from both the network and the host, filter incoming data, and extract interesting and potentially valuable (e.g., statistical) information which is needed to construct an appropriate event. At the detection layer, different detectors, e.g., classifiers trained with machine learning techniques such as support vector machines (SVM) or conventional rule-based systems such as Snort, assess these events and search for known attack signatures (misuse detection) and suspicious behavior (anomaly detection). In case of attack suspicion, they create alerts which are then forwarded to the alert processing layer. Alerts may also be produced by firewalls (FW) or the like. At the alert processing layer, the alert aggregation module has to combine alerts that are assumed to belong to a specific attack instance. Thus, so-called meta-alerts are generated. Meta-alerts are used or enhanced in various ways, e.g., scenario detection or decentralized alert correlation. An important task of the reaction layer is reporting.

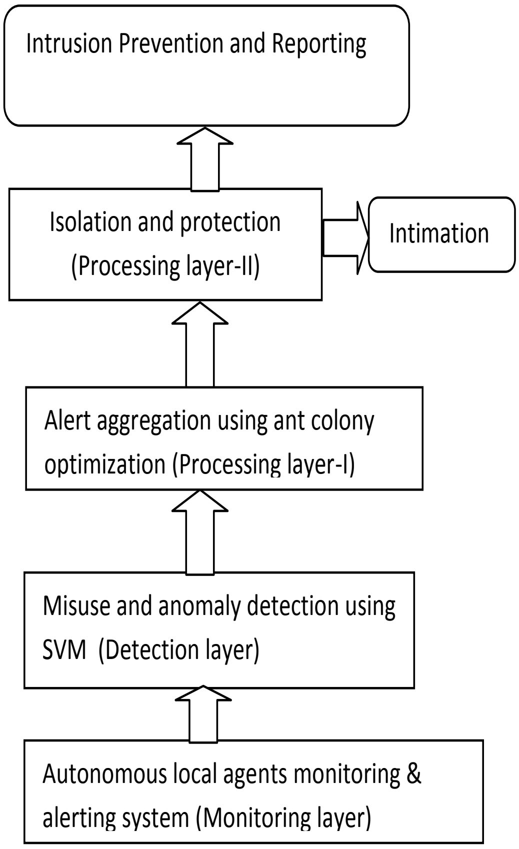


Fig.2:Architecture of proposed IDS

A. Monitoring layer: The individual multiple agents located on each host monitors for any malicious or anomaly or deviation from normal activities. If any misbehavior, the details will be intimated to detection layer. Whenever a node wants to transfer information to another node, it broadcasts the message to its neighboring nodes. The agent also gathers neighboring nodes information. It then calls the SVM classifier to find out the attacks with the help of trained test data.

B. Detection Layer: SVM classifier compares the data submitted by local agents with trained test data and alerts the attack if any.

C. Processing layer-1: The alerts made by the detection layer are aggregated using ant colony optimization. The pseudo code is

```
procedure Alert_Heuristic
   while(not_termination)
     generateSolutions()
     daemonActions()
     Updatedatabase()
   end while
end procedure
```

D. Processing layer-2: The identified node is isolated and prevented from further attack. The message is communicated to all the remaining nodes to avoid communication and asked to update the local agent's database about the attack.

E. Intrusion prevention: The characteristics of new attack is identified and analyzed for prevention of such attacks in future. Proper report also created for further reference.

IV SIMULATIONS AND FUTURE WORK

The proposed system is verified using the network simulator software NS-2 networking simulator. The simulated environment is as follows:

TABLE I. SIMULATED ENVIRONMENT

Property	Value
Network shape	500 meter X 500 meter
Radio Range of each node	160-220 meters
Node Selection	Random
Base Station Moment	Random
Topological Model	Multi hop hierarchical
Speed of each node	5 meters/second
Transmission Capacity	2 Mbps
Total flows	20-30
Set node count	50
Average transmission per flow	3 packets per second
Testing execution time	1 minute

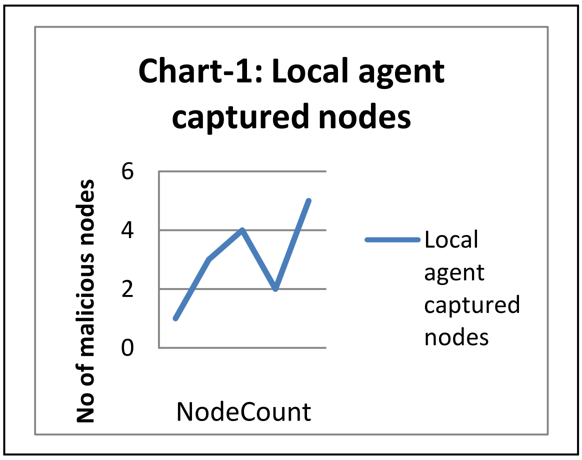
V RESULT AND FINDINGS

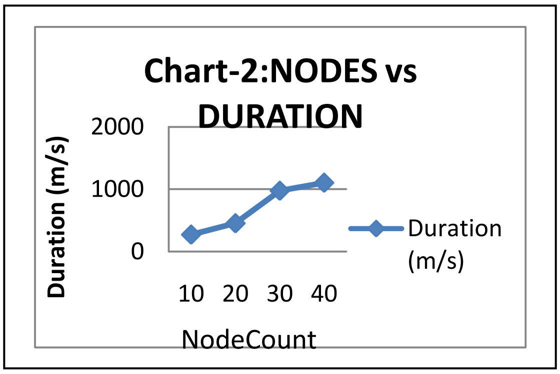
The result shows the following findings:

- When number of nodes increases, the effectiveness of local agents decreases (Chart-1). Until number of nodes reaches 40, 100% detection accuracy found. When nodes count reaches 50, only 80% of malicious nodes were detected.

- The time duration is not increased proportionally in same ratio with increase the node count (Chart-2). The analysis duration for 20 nodes is not doubled the duration for 10 nodes.

S.No	No of Nodes	Malicious Nodes	Local agent captured nodes	Duration (m/s)
1.	10	1	1	271
2.	20	3	3	453
3.	30	4	4	976
4.	40	2	2	1105
5.	50	6	5	1343





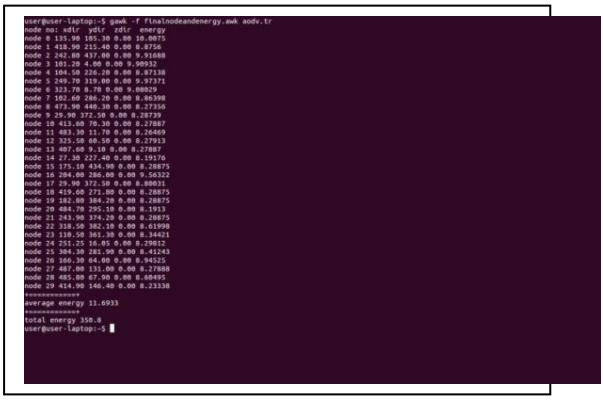


Fig.3:NS2 Screenshot-finding destination

VI CONCLUSION

Design of an IDS with localized agents with monitoring and preventive control for both hosts and the whole network faces many challenges. Disentangled design with high accuracy are the main factors in IDS design. This research work initiated an agent based IDS which satisfies the above mentioned criteria. This work can be further developed in future for android mobile and direct wifi devices.

REFERENCES

[1] Dokurer, S. Ert, Y.M. ; Acar, C.E." Performance analysis of ad-hoc networks under black hole attacks", Proceedings. IEEE. pp. 148 – 153, 2007

[2] Deng, H., Li, W., Agrawal, D., "Routing Security in Wireless Ad Hoc Networks" IEEE Communication Magazine (October 2002) pp. 70-75

[3] Al-Shurman, M., Yoo, S., Park, S., "Black hole Attack in Mobile Ad Hoc Networks", ACM Southeast Regional Conference (2004) pp. 96-97

[4] Mishra, A., Nadkarni, K., Patcha, A., "Intrusion detection in wireless ad-hoc networks", IEEE Wireless Communications, February 2004, pp. 48-60.

[5] Abdelgadir, A.T., M. Ahmed, A.S.K. Pathan, M.A. Abdullah and S. Haseeb, 2011. Performance analysis of a highly available home agent in mobile networks. Am. J. Applied Sci., 8: 1388-1397. DOI:10.3844/ajassp.2011.1388.1397

[6] Bose, S., S. Bharathimurugan and A. Kannan, 2007.Multi-layer integrated anomaly intrusion detection system for mobile adhoc networks. Proceedings of the International Conference on Signal Processing, Communications and Networking, Feb. 22-24, IEEE Xplore Press, Chennai, pp: 360-365. DOI:10.1109/ICSCN.2007.350763

[7] Chuan-Xiang, M. and F. Ze-Ming, 2009. A novel intrusion detection architecture based on adaptive selection event triggering for mobile ad-hoc networks. Proceedings of the 2nd International Symposium on Intelligent Information Technology and Security Informatics, Jan. 23-25, IEEE Xplore Press, Moscow, pp: 198-201. DOI:10.1109/IITSI.2009.54

[8] Farhan, A.F., D. Zulkhairi and M.T. Hatim, 2008.Mobile agent intrusion detection system for Mobile Ad Hoc Networks: A non-overlapping zone approach. Proceedings of the 4th IEEE/IFIP International Conference on Internet, Sept. 23-25, IEEE Xplore Press, Tashkent, pp: 1-5. DOI: 10.1109/CANET.2008.4655310

[9] Jacoby, G.A. and N.J. Davis, 2007. Mobile host-based intrusion detection and attack identification. IEEE Wireless Commun., 14: 53-60. DOI: 10.1109/MWC.2007.4300984

[10] Jha, S., K. Tan and R. Maxion, 2001. Markov chains, classifiers and intrusion detection. Proceedings of the 14th IEEE Computer Security Foundations Workshop, Jun. 11-13, IEEE Xplore Press, pp: 206-219. DOI:10.1109/CSFW.2001.930147

[11] Kominos, N. and C. Douligeris, 2009. LIDF: Layered intrusion detection framework for ad-hoc networks. Ad Hoc Networks, 7: 171-182. DOI: 10.1016/j.adhoc.2008.01.001

[12] Lauf, A., R.A. Peters and W.H. Robinson, 2010. A distributed intrusion detection system for resource constrained devices in ad-hoc networks. Elsevier J. Ad Hoc Network., 8: 253-266. DOI:10.1016/j.adhoc.2009.08.002

[13] Ms Priyanka P Kulkarni, 2015, A Survey on Secure Intrusion Detection System for MANET, International Journal of Advanced Research in Computer Science and Software Engineering, 5:3-4.

[14] Vishnu Balan E, Priyan M K, Gokulnath C, Prof.Usha Devi G, 2015, Fuzzy Based Intrusion Detection Systems in MANET, 2nd International Symposium on Big Data and Cloud Computing (ISBCC'15), Elsevier ScienceDirect, Procedia Computer Science 50 (2015) 109 – 114.

[15] J. Godwin Ponsam, R. Srinivasan, 2014, Multilayer Intrusion Detection in MANET, International Journal of Computer Applications (0975 – 8887) 98: 20