Journal of Computer Science 10 (6): 970-975, 2014
ISSN: 1549-3636

doi:10.3844/jcssp.2014.970.975 Published Online 10 (6) 2014 (http://www.thescipub.com/jcs.toc)

A MOBILE AGENT BASED INTRUSION DETECTION SYSTEM ARCHITECTURE FOR MOBILE AD HOC NETWORKS

[1]Binod Kumar Pattanayak and [2]Mamata Rath

[1]Department of Computer Science and Engineering,
Institute of Technical Education and Research, Siksha 'O' Anusandhan University, Bhubaneswar, Odisha, India
[2]Department of MCA, C. V. Raman Computer Academy, Bhubaneswar, Odisha, India

Received 2013-12-20; Revised 2013-12-26; Accepted 2014-01-28

ABSTRACT

Applications of Mobile Ad Hoc Networks (MANETs) have become extensively popular over the years among the researchers. However, the dynamic nature of MANETs imposes a set of challenges to its efficient implementation in practice. One of such challenges represents intrusion detection and prevention procedures that are intended to provide secured performance of ad hoc applications. In this study, we introduce a mobile agent based intrusion detection and prevention architecture for a clustered MANET. Here, a mobile agent resides in each cluster of the ad hoc network and each cluster runs a specific application at any point of time. This application specific approach makes the network more robust to external intrusions directed at the nodes in an ad hoc network.

Keywords: Ad Hoc Network, MANET, IDS, Mobile Agent

1. INTRODUCTION

Security issues impose various challenges to applications on a MANET. Dynamic nature of MANET makes it even more challenging. Intrusion detection and prevention, as one of the major security issues, has been the centre of investigation among most of the researchers of late. Several Intrusion Detection System (IDS) architectures have been proposed in the literature. In this study, we introduce an IDS architecture for clustered ad hoc networks. In this proposed architecture, each cluster in the network implements a Mobile Agent (MA) that caters all the functionalities including intrusion detection and prevention measures during the entire lifetime of the network. In difference with all other proposed IDS Architectures, it assumes all the activities in a cluster to be controlled by a dedicated MA. In addition, each cluster runs a specific application at any point of time and can switch over to another application after accomplishment of the current one. This architecture can be hopefully implemented using network simulators such as NS-2 or Qualnet in order for justification of optimal intrusion detection and prevention in a clustered ad hoc network.

The rest of the study is organized as follows.

2. RELATED WORK

A huge spectrum of research works on IDS architectures is evident from the literature. Jacoby and Davis (2007) proposed a two-stage stand alone IDS architecture, where the malicious activities across an ad hoc network can be successfully identified by continuously monitoring the battery power consumptions in the network. However, the authors do not consider the packet level intrusion in their proposed architecture and this architecture can induce attacks related to power consumption only, although the authors claim that 99% of intrusions can be successfully identified by it. IDS architecture proposed by Nadkarni and Mishra (2004), relies on a compound detection policy for reducing the false positives during

Corresponding Author: Binod Kumar Pattanayak, Department of Computer Science and Engineering,
Institute of Technical Education and Research, Siksha 'O' Anusandhan University, Bhubaneswar, Odisha, India

anomaly detection, where thresholds are adjusted to determine malicious behavior. A stand-alone IDS architecture for resource-constrained MANETs was proposed by Lauf *et al*. (2010) that comprises of two separate detection engines on every node: (i) Maxima Detection System (MDS), meant for rapid identification of potential threats and calibration of the second detection engine; (ii) Cross-Correlative Detection System (CCDS), used for identification of malicious behaviours. Wang *et al*. (2009) proposed a cooperative IDS architecture which includes a detection engine for anomaly detection that solely relied on social network analysis strategies. This approach imposes less computational overhead. Another cooperative IDS architecture devised by Bose *et al*. (2007) assumes deployment of three detection engines on every node: (i) MAC layer detection engine; (ii) routing layer detection engine; and (iii) application layer detection engine. Implementation of multi-layer detection policy facilitates enhancement in detection accuracy since attacks at upper layers lead to legitimate events at the lower layers and vice versa. Effectiveness of this architecture was successfully established by the authors via extensive simulations using GloMoSim (Zeng *et al*., 1998). An IDS architecture with a two-tier detection policy (one for local detection and one for global detection), devised by Razak *et al*. (2008), implemented two detection engines at the first tier. The first tier collects local audit data and verifies with signature-based method. If it fails in anomaly detection, then the second engine is calibrated. If both of these engines are unable to detect an anomaly, then the engine at the second tier is triggered that collects audit data from its neighbours, called as friends (trusted nodes) and performs anomaly detection in the same manner as the first tier using signature-based policy. However, this architecture is identified to be more complex and incurs significant computational load. With an intention to reduce battery consumption along with anomaly detection, a cooperative IDS architecture was addressed by Ramachandran *et al*. (2008) using light weight agents. A routing anomaly detection IDS architecture was suggested by Sun *et al*. (2003) that successfully identifies routing disruptions. It uses frequent updates in the routing tables and performs anomaly detection using two parameters: (i) Percentage of Changes in Routing entries (PCR) and (ii) Percentage of Changes in number of Hops (PCH). Here, the authors use a modified Markov Chain anomaly detection (Jha *et al*., 2001) technique in order for performing anomaly detection. However, this approach is incapable of determining all possible attacks as it concentrates only on routing anomalies. Furthermore, an improved anomaly detection architecture was proposed by Sun *et al*. (2007), which implemented another detection engine in the previously discussed architecture and it relies on regulative thresholds, consequently addressing most of its drawbacks. Kominos and Douligeris (2009) proposed a cooperative IDS architecture that incorporates a multi-layered detection strategy in order for detection of malicious behaviours. In this architecture, three modules are deployed on every host: (i) collection module for collecting audit data; (ii) detection module for anomaly detection; and (iii) alert module for raising an alarm. A hierarchical IDS architecture, using a modular approach to design, was proposed by Chuan-Xiang and Ze-Ming (2009) that can be used for clustered ad hoc networks, where a node with maximum battery power can be elected as cluster head. Each node in this approach comprised of four modules: (i) network detection module for network packet monitoring within a cluster; (ii) local detection module for generating alert after identification of malicious activities; (iii) resource management module for continuously monitoring battery power of the cluster head and notify the monitoring state managing module in case it goes below a predefined threshold; and (iv) monitoring state managing module that monitors if the network detection module is active. Otrok *et al*. (2008) devised another hierarchical IDS architecture aimed at balancing resources among the nodes of the network within a cluster, emerging from intrusion detection procedures. Two IDS architectures were proposed by Marchang and Datta (2008): (i) Algorithm for Detection in a Clique (ADCLI) and (ii) Algorithm for Detection in a Cluster (ADCLU). ADCLI is similar to ADCLU with the only difference that within ADCLI, each node in it has every other node in the clique as the neighbor. Here, intrusion detection in each cluster/clique is performed independently and the cluster/clique head, on identification of intrusion, notifies other clusters/cliques to trigger intrusion detection process. An optimal hierarchical IDS architecture addressed by Manousakis *et al*. (2008) using a hierarchical tree-based structure that aggregates detection data upwards, i.e., from leaf nodes to the root node, during intrusion detection procedure. This approach provides a more robust structure and intrusion can be determined at each level of the tree. Intrusion detection is carried out for attacks affecting only the routing infrastructure in the clustered IDS architecture proposed by Deng *et al*. (2006). Mishra *et al*. (2009) used an application-specific approach to identification of malicious activities within an ad hoc network, where a node can be blocked from forwarding and sending packets if it violates the service agreement of the application running in it. We have incorporated the same approach in our proposed model. Pattanayak *et al*. (2009) proposed a distributed cluster scheme, where an ad hoc network can be split into grid clusters and a cluster head can be elected with respect to available battery power. In our approach, we too incorporate the grid clustering approach and similar method for cluster head election procedure. Farhan *et al*. (2008) propose a mobile agent based IDS architecture aimed at decreasing the number of false positives generated in a cooperative intrusion detection system. Sen (2010) proposes a distributed cluster based IDS architecture for addressing the security vulnerabilities and detection of attacks. It uses a dynamic hierarchical approach, where the intrusion data collected by nodes, are incrementally aggregated, analyzed and reduced in volume as it flows upwards to the cluster head and the cluster heads communicate among themselves to perform cooperative intrusion detection. Nakeeran *et al*. (2010) have come up with an agent based anomaly IDS architecture that uses agents and data mining techniques for prevention of intrusion.

We also investigated a set of intrusion detection algorithms devised by variety of authors that can be helpful to implement/evaluate intrusion detection process. Evaluation of IDS architectures can be achieved using the linear classifier, Gaussian mixture model and Support vector machine approaches, as suggested by Mitrokotsa *et al*. (2008). Dynamic Source Routing (DSR) protocol was modified by Nuruzzaman *et al*. (2007) with an intention to enhance the security measures and accommodate intrusion detection in an ad hoc network. Bose *et al.* (2007) came up with a novel intrusion detection algorithm that takes into account intrusion detection at three layers: MAC layer, routing layer and application layer. A cross layer intrusion detection algorithm is proposed by Shrestha *et al.* (2010) in order to enhance detection accuracy, where malicious nodes can be successfully discovered and different Denial Of Service (DOS) attacks can be identified and information across different layers of protocol stack can be explored. Rahuman and Athisha (2012) propose a reconfigurable hardware architecture for Network Intrusion Detection System (NIDS) that combines Ternary Content Addressiable Memory (TCAM) and Bit Vector (BV) Algorithm, called BV-TCAM architecture implemented for Field Programmable Gate Array (FPGA) based NIDS. Abdelgadir *et al.* (2011) use a Home Agent (HA) in order for failure detection and recovery in Mobile IPv6 (MIPv6) networks running real time applications.

3. OUR PROPOSED IDS ARCHITECTURE

Our proposed architecture is depicted in **Fig. 1**. The ad hoc network is split into grid clusters. The number of clusters in this architecture is assumed to be a power of two. Each cluster is assigned with a cluster ID. Zone of the node is designated as Cluster Head (CH) and all other nodes as Cluster Members (CM). Election of a CH is carried out with respect to the available battery power in the node at the point of initiation of an application. Thus, the node with maximum battery power available is elected as the CH.

We have taken the following assumptions in our proposed model:

- Each cluster runs a specific application at any point of time
- The CH does not change during the entire lifetime of the current application
- All communications among the nodes in a cluster are performed via the CH
- Once the application resumes, no node can leave the cluster until the application terminates its job

The functioning of our model is detailed below. A dedicated Mobile Agent (MA) is incorporated in each cluster. The internal components of MA are shown in **Fig. 2**. MA comprises of four modules: Registration Module (RM), Service Agreement (SA), Detection Module (DM) and Prevention Module (PM). During the deployment of the network and during initiation of a new application, all the nodes (CH and CMs) in the cluster need to register with the MA and MA maintains a list of nodes in the cluster in RM. Then each node needs to accept the SA that complies with the specific requirements of the application. During the entire lifetime of the application, intrusion Detection Module (DM) in MA, monitors each packet routed through the CH. The format of the packet is demonstrated in **Fig. 3**. It includes source address, destination address, application ID, packet length, data field and CRC for error detection. A threshold for the packet length is predefined for each application. DM compares the source address, destination address, application ID and packet length. If a mismatch occurs in source and destination addresses that can be verified with RM, then MA informs CH to drop the packet and to block the respective node following which the node is debarred from taking part in communication. If the application ID does not match or the packet length exceeds the threshold, then only the packet is dropped by the CH.

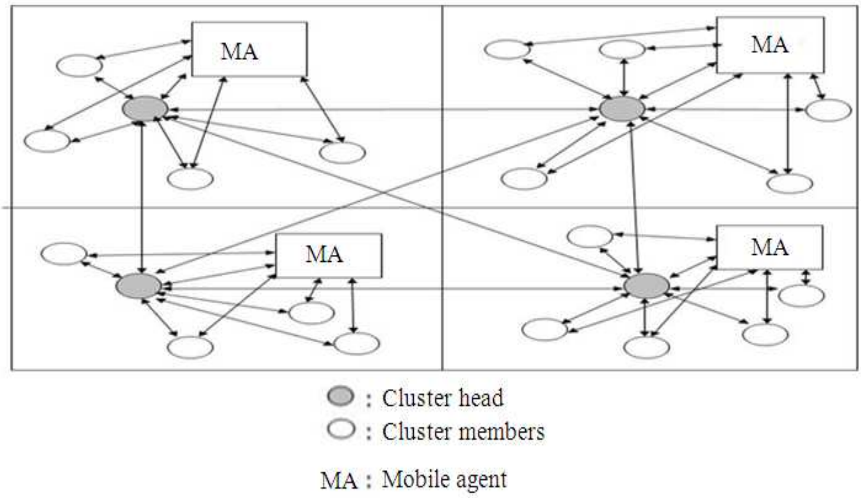

Fig. 1. Our proposed IDS architecture for grid clustered ad hoc network

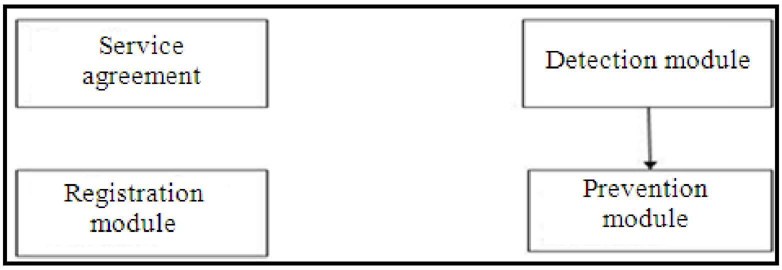

Fig. 2. Mobile agent

Source address	Destination address	Application id	Data	Packet length	CRC

Fig. 3. Packet format

In both of these cases, an intrusion is inferred and the intrusion Prevention Module (PM) is triggered to take necessary actions.

In addition to the above, inter cluster communications are permissible here. For example, a cluster running a multimedia application, may require the service of a file sharing application running in another cluster. During such inter cluster communications, the CHs exchange packets that are monitored by the respective MAs. A packet can be sent from a cluster to the desired cluster only if the MA of the sending cluster approves it, discarded otherwise. After receiving a packet from another, if the destination address does not match with the list of registered nodes in the receiving cluster, then MA informs CH to drop the packet and at the same time, receiving CH notifies the sending CH regarding this event. After the accomplishment of the current application, nodes of the cluster can move out to another cluster and new nodes from other clusters may join the cluster. Hence, the registration process is again facilitated by MA for a desired new application and accordingly, the new SA is incorporated. Subsequently, new application ID must be added to the packets of the newly initiated traffic.

The advantages of our model can be summarized as:

- The architecture is simplified enough to implement
- A much higher rate of intrusion detection can be achieved that is to be established in future through extensive simulations

- The model is applicable to a variety of applications
- Simplified communication since no multi-hop communication is allowable
- Intrusion detection procedure is simple enough as the DM monitors only the CH

The drawbacks may be concluded as:

- The MA may happen to be overloaded with multiple functionalities that may lead to errors
- It may not optimally run real time applications with strict time bounds as the communication is time consuming for the reason that all packets are routed through the CH
- Deployment cost may appear to be very high and may not conform to the needs of a customer

4. CONCLUSION

Intrusion detection in localized ad hoc networks may very often impose several challenges to secured communication. Simplified design and optimal rate of detection are the key factors to deployments of such networks. In this study, we introduce a mobile agent based IDS architecture that can cater to these requirements. However, the effectiveness of this architecture needs to be tested through extensive simulations with a variety of applications, which is our anticipated future work in this context.

5. REFERENCES

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

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

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

Deng, H., R. Xu, J. Li, F. Zhang and R. Levy *et al*., 2006. Agent-based cooperative anomaly detection for wireless ad hoc networks. Proceedings of the 12th Conference on Parallel and Distributed Systems, Jul. 12-15, IEEE Xplore Press, Minneapolis, pp: 1521-9097. DOI: 10.1109/ICPADS.2006.23

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

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

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

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

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 Netw., 8: 253-266. DOI: 10.1016/j.adhoc.2009.08.002

Manousakis, K., D. Sterne, N. Ivanic, G. Lawler and A. McAuley, 2008. A stochastic approximation approach for improving intrusion detection data fusion structures. Proceedings of the IEEE Military Communications Conference, Nov. 16-19, IEEE Xplore Press, San Diego, pp: 1-7. DOI: 10.1109/MILCOM.2008.4753175

Marchang, N. and R. Datta, 2008. Collaborative techniques for intrusion detection in mobile ad-hoc networks. Elsevier Ad Hoc Netw., 6: 508-523. DOI: 10.1016/j.adhoc.2007.04.003

Mishra, M.K., B.K. Pattanayak and A.K. Jagadev, 2009. Self centric protected ad hoc networks. Int. Advancements Comput. Technol., 1: 110-121.

Mitrokotsa, A., M. Tsagkaris and C. Douligeris, 2008. Intrusion detection in mobile ad hoc networks using classification algorithms. Proceedings of the 7th Annual Mediterranean Ad Hoc Networking Workshop, Palma de Mallorca, Jun. 25-27, Spain, pp: 133-144. DOI: 10.1007/978-0-387-09490-8_12

Nadkarni, K. and A. Mishra, 2004. A novel intrusion detection approach for wireless ad hoc networks. Proceedings of the IEEE Wireless Communications and Networking Conference Mar. 21-25, IEEE Xplore Press pp: 831-836. DOI: 10.1109/WCNC.2004.1311294

Nakeeran, R., A. Aruldoss and R. Ezumalai, 2010. Agent based anomaly intrusion detection system in ad hoc networks. Int. J. Eng. Technol., 2: 52-56.

Nuruzzaman, A.T., S. Haque and M.N. Masum, 2007. Modification of DSR and its implementation in ad hoc city. Proceedings of the 10th international Conference on Computer and Information Technology, Dec. 27-29, IEEE Xplore Press, Dhaka, pp: 1-5. DOI: 10.1109/ICCITECHN.2007.4579445

Otrok, H., N. Mohammed, L. Wang, M. Debbabi and P. Bhattacharya, 2008. A game-theoretic intrusion detection model for mobile ad hoc networks. Comput. Commun., 31: 708-721. DOI: 10.1016/j.comcom.2007.10.024

Pattanayak, B.K., A.K. Jagadev and M.K. Mishra, 2009. A distributed cluster scheme for bandwidth management in multi-hop MANETs. Int. J. Comput. Sci. Netw. Security, 9: 220-226.

Rahuman, A.K. and G. Athisha, 2012. Reconfigurable hardware architecture for network intrusion detection system. Am. J. Applied Sci., 9: 1618-1624. DOI: 10.3844/ajassp.2012.1618.1624

Ramachandran, C., S. Misra and M. Obaidat, 2008. FORK: A novel two-pronged strategy for an agent based intrusion detection scheme in ad-hoc networks. Elsevier Comput. Commun., 31: 3855-3869. DOI: 10.1016/j.comcom.2008.04.012

Razak, S.A., S.M. Furnell, N.L. Clarke and P.J. Brooke, 2008. Friend-assisted intrusion detection and response mechanisms for mobile ad hoc networks. Elsevier Ad Hoc Netw., 6: 1151-1167. DOI: 10.1016/j.adhoc.2007.11.004

Sen, J., 2010. An intrusion detection architecture for clustered wireless ad hoc networks. Proceedings of the 2th International Conference on Computational Intelligence, Communication Systems and Networks, Jul. 28-30, IEEE Xplore Press, Liverpool, pp: 202-207. DOI: 10.1109/CICSyN.2010.51

Shrestha, R., K.H. Han, D.Y. Choi and S.J. Han, 2010. A novel cross layer intrusion detection system in MANET. Proceedings of the 24th IEEE International Conference on Advanced Information Networking and Applications, Apri. 20-23, IEEE Xplore Press, Perth, pp: 647-657. DOI: 10.1109/AINA.2010.52

Sun, B., K. Wu and U.W. Pooch, 2003. Routing anomaly detection in mobile ad hoc networks. Proceedings of the 12th International Conference on Computer Communications and Networks, Oct. 20-22, IEEE Xplore Press, pp: 25-31. DOI: 10.1109/ICCCN.2003.1284145

Sun, B., K. Wu, Y. Xiao and R. Wang, 2007. Integration of mobility and intrusion detection for wireless ad hoc networks. Wiley Int. J. Commun. Syst., 20: 695-721. DOI: 10.1002/dac.853

Wang, W., H. Man and Y. Liu, 2009. A framework for intrusion detection systems by social network analysis methods in ad hoc networks. Wiley Security Commun. Netw., 2: 669-685. DOI: 10.1002/sec.108

Zeng, X., R. Bagrodia and M. Gerla, 1998. GloMoSim: a library for parallel simulation of large-scale wireless networks. Proceedings of the 12th Workshop on Parallel and Distributed Simulations, May 26-29, ieee Xplore Press, Banff, pp: 154-161. DOI: 10.1109/PADS.1998.685281