Available online at www.sciencedirect.com

ScienceDirect

Procedia Computer Science 46 (2015) 1203 – 1208

Procedia Computer Science

International Conference on Information and Communication Technologies (ICICT 2014)

A Distributed Self-Adaptive Intrusion Detection System for Mobile Ad-hoc Networks using Tamper Evident Mobile Agents

Deepa Krishnan[a,]*

[a]*Pillai Institute of Information Technology Media Studies and Research Centre,New Panvel,Mumbai,410206,India*

Abstract

This paper brings forth a distributed self adaptive intrusion detection system (IDS) based on programmable mobile agents which can act as a key line of defense against major security attacks. The proposed intrusion detection model is organized as a combination of the two trends in IDS; the rule based and the behavior based scheme. Also this model draws out the merits of both the host based and networks based IDSs and deploy them wisely considering the critical features of MANETs. In contrast to many proposed and implemented IDSs, this is an efficient framework conscious of the inherent constraints of MANETS and are self adaptive in nature. In addition to this, the use of light weight mobile agents provide a low overhead mechanism which in turn is well suited to MANET characteristics. Through this paper, an attempt to improvise the mobile agents is done by making it tamper evident which is very essential as the agents can be compromised and thereby turning all the efforts of the IDS futile.

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)

Keywords: Mobile Ad-hoc Networks, adaptability, mobile agents, Intrusion detection system, tamper evident;

1. Introduction

In recent decades, MANETs have been widely used in many critical applications and with wide spread usage security became a challenging problem for this prominent technology. This is mainly due to the design properties of ad hoc networks like peer-to-peer multi-hop infrastructure-less network architecture, shared wireless medium,

* Corresponding author. Tel.: +91977-342-3043; fax: +0-222-748-3208.
E-mail address: dkrishnan@mes.ac.in

Peer-review under responsibility of organizing committee of the International Conference on Information and Communication Technologies (ICICT 2014)
doi:10.1016/j.procs.2015.01.034

stringent power and bandwidth constraints and above all, the highly dynamic network topology with frequently changing channel access and routing decisions. Mobile ad hoc networks face additional security problems compared to the traditional infrastructure based wired networks. Thus, efficient security mechanisms are the need of the hour. However, we should remember the fact that most of the security techniques designed and tested for wired networks seem to be unsuitable for ad hoc networks. Hence, when designing any security technique, the key features of MANETS should be well considered. This paper concentrates on Intrusion Detection System as it is always a major line of defense against attacks and a widely accepted proactive defense strategy.

This proposed scheme is designed considering dynamic nature of MANETs and its various associated constraints. It provides a light weight, low overhead Intrusion Detection Scheme which is based on programmable mobile agents. This direction draws benefits from both the behavior based and rule based schemes. The behavior based approach is in turn coupled with efficient fuzzy logic training schemes to significantly reduce the false positives and increase detection rates. The highlight of this work is that it ensures the security of its agents by making it tamper evident. The beauty and effectiveness of this approach is that the entire IDS scheme revolves around the use of programmed and dynamic mobile agents to achieve all the functionalities.

2. Background Study

2.1. Study of Various IDS Schemes

One commonly used IDS classification scheme is the behavior based detection which is built on a long term monitoring and classification of what is expected/normal or abnormal. This scheme is very challenging to implement due to the dynamic nature resulting in random communication patterns. Another approach is the rule based model which requires maintenance of an extensive database of all attack patterns and needs to be periodically updated at each node. This approach cannot be relied alone as it incurs more computational cost and may not be effective in detecting new attacks.

Another direction in the IDS classification is the Distributed Vs Centralized schemes. A distributed IDS scheme uses cooperative detection strategies to determine an attack whereas in Centralized approach decision is taken unilaterally. There is one more classification related to the distribution of functionality as flat and hierarchical approach. In the flat architecture every node in the network shares same responsibilities and tasks in intrusion detection and decision making whereas in the hierarchical architecture, nodes have varying functionalities with one root node making control decisions.

2.2. Related Works

Several efforts has been made in the design of Intrusion detection systems for MANETs, however most of them couldn't bring out an efficient and reliable scheme which covers all aspects of MANET security. One of the pioneering works in this field is[1] by Zhang and Lee in which they have described a distributed and cooperative intrusion detection system for MANETs. In this model, they have used a flat architecture and the IDS agents deployed in the mobile nodes are given equal importance. However, each of these look for malicious activities in their respective nodes and it is only in instances of inconclusive evidences that intrusion detection is performed using cooperative voting method. Intrusion detection is done in a distributed and cooperative manner, however at the core it functions in a flat architecture.

Another related architecture is suggested by Smith in his mobile-agent based IDS architecture[2] for wireless ad-hoc networks. The work by Smith is also in a similar direction as that of the previous one wherein a flat architecture and distributed co-operative manner for intrusion detection is used. The difference between this model and the one explained in [1] is that it uses agents that are static and follow RPC schemes for communication whereas Smith make use of mobile agents. The potential benefits of using mobile agents like reduced network latency and communication overhead and improved scalability are very well explained in [3, 4 ,5].

In [6], the author presents an intrusion detection system which makes use of SNMP data in MIBs as audit sources. Another mobile agent based IDS architecture is proposed for MANETs in[7]. In contrast to [1, 2] this scheme follows a hierarchical architecture for intrusion detection.

Apart from all this, my proposed scheme is greatly inspired by the clustered network monitoring node selection algorithm proposed by Kachirski and Guha[7] and secure leader election algorithm optimized for power saving designed by M.Darji and B.Trivedi[8]. The paper[7] describes an algorithm to logically divide a mobile network into clusters, each having its own cluster head for monitoring packets within the cluster. However this scheme suffers from the potential drawback of large number of broadcasts and signature verifications that need to be performed in all the nodes for gathering resource information from neighbouring nodes. Hence in my proposed work I have drawn the concept of logical division of mobile networks from[7] and the idea for selection of cluster head from the work[8] which is described as follows. The research work by Darji and Trivedi brings forth a leader selection algorithm that reduces the overall battery and bandwidth consumption leading to efficiency and power saving very much suited for resource constrained wireless sensor networks. This idea has been used in my model for network node selection for deploying the various network monitoring agents.

Finally, the work by Yinghua Guo and Steven Gordon[9] is worth mentioning. The novelty of this approach is the use of attack tolerant mobile IDS agents which are roaming in the network. However, less efforts are made to reduce the number of false positives and to detect new attacks.

2.3. Comparative Analysis of the Related Works and Motivation for Proposed Scheme

In this section, I have attempted to make broad analysis of the related approaches in the light of the various requirements like Effectiveness, Efficiency, Self-Security and Adaptability/Self Learning.

Effectiveness: The research works [1, 2] follow a flat architecture for intrusion detection and in[7] a hierarchical architecture. The effectiveness of an IDS model is highly dependent on the ID algorithm used and the algorithm execution method. Even though [1, 2] uses distributed and cooperative approach, it suffers from the drawback of flat architecture. Any flaw or functional incorrectness of participating nodes can severely delimit the effectiveness in a flat and centralized architecture. Because of this aspect, a hierarchical and modular approach will be a better choice for rendering effective intrusion detection.

Efficiency: An efficient IDS model should minimize the use of the network and host resources like CPU power, bandwidth and battery power. A flat architecture compared to the hierarchical scheme suffers from potential draw backs in the following two aspects. There is considerable bandwidth consumption related to exchange of data between all participating nodes and over utilization of node resources due to duplicated ID functions in every node rather than the specialized task distribution in the hierarchical scheme.

Self Security and Adaptability: An IDs scheme designed for MANETs should be immune to attacks and should be capable of learning new attacks in the dynamic and heterogeneous MANET environment. In addition to this, there can be chances of IDS getting corrupted due to falsified or malicious inputs.

In short, all these factors should be considered while designing and implementing an IDS scheme for mobile ad hoc networks. As per analysis, it can be seen that none of the IDS models discussed in the related works have completely met the above requirements. This motivated me to design a distributed intrusion detection system for MANETs using secure mobile agents. The proposed scheme tries to cover up the demerits of the existing systems by making use of the combination of rule-based and behavior based schemes. Above all there is a dynamic learning module which uses advanced artificial neural networks and fuzzy logic algorithm to develop new attack libraries. This can help in reducing false positives to a great extent and to identify new attack patterns.

Apart from all these, in my ongoing work I have made a modification to the cluster selection algorithm described in[8] , by selecting few other supporting nodes to the main cluster head to deploy the various network monitoring agents. This is done to make sure that the network monitoring nodes deployed covers the entire span of the network. Other supporting nodes are selected by the main cluster head depending on the remaining battery power available in nodes. The number of such nodes selected depends on the size of the cluster.

.

3. Architecture and Working of Proposed Distributed IDS

The working of the proposed IDS can be divided into two phases: A) Initialization Set up and Learning Phase B) Agent Deployment and Intrusion Detection

A) Initialization Set up and Learning Phase: In the initialization and set up phase, collector agents are deployed to collect data from different audit sources like network, host or application level. This initial raw data collected will be stored in the primary database of the test bed and then fed to a pre processor for filtering. The filtered and pre processed data will be used for various attack rule formation. In this stage, the processed data are organized as atomic events which can further be combined to create complex attack rules. This can be effectively done through pattern matching algorithm and thus gradually an attack library is being setup. The attack library is continuously built on a learning module implemented as part of the test bed. Initially the system tries to build up rules for simple flooding attacks and these rules serve as the building blocks for constructing rules for other network layer attacks like worm hole, black hole and grey hole attacks. Thus a comprehensive attack database is being built up.

While the learning stage is in progress, the clustered node selection algorithm is used to select the nodes to deploy the network monitoring agents. As the physical topology changes, the cluster nodes are dynamically updated. Thus in a cluster, few nodes monitor the network and other nodes monitor system level events to look for intrusions. This scheme helps in reducing the power consumption in the nodes as every node has to perform a simple subset of the intrusion detection tasks.

B) Agent Deployment and Intrusion Detection: The proposed intrusion detection system is built using a hierarchical system of multi agent architecture. The following types of agents are mainly used in the proposed system.

Network Monitoring Agents: Only few nodes in the cluster will be deployed with the agent for monitoring network packets. These agents are responsible for collecting the network related parameters necessary for the IDS to function.

Host Monitoring Agents: Every node on the mobile ad-hoc network is monitored internally by a host monitoring agent. It monitors system-level and application level activities.

*Decision Making Agent*s: Every node makes decisions regarding intrusions based on individual threshold threat level assigned. If there is any ambiguity it can take suggestion from learning module to arrive at a decision. Learning module has the reasoning logic using the certainty factor theory. Decision making agents make use of simple associative rules to figure out an abnormal behavior.

Database Agents: Database agents are of 3 types. Primary database, which is a part of the learning module which continuously collects information about the network and the host through mobile surveillance agents; which are sent by the learning module at scheduled intervals. The host information data base and network information database agents store the host and network related events and logs respectively. Also the database has a predetermined attack rule base which will be periodically updated whenever mobile agents visit a node.

Communication Agents: This agent is built as part of both the host and network ids. Whenever a roaming/mobile agent visits any node, communication agent reads information from the mobile agent and if found to be a new attack rule, it will be added to the attack database by the database agent.

Alert Agents: On detection of any new attack or suspicious event, any node can issue an alert agent which notifies the learning module. The learning module can verify the trust worthiness and authenticity of the alert through the inference engine. If it finds the event to be a new attack, it notifies other nodes also about the new attack and updates the attack database.

4. Experiment Setup and Implementation Details

The prototype system is being developed using WADE 3.3, JADE extension. JADE framework provides both the libraries to develop the various agent modules and run-time environment provides the essential services required for executing the agents. There are few other key features of JADE that makes it a better choice for development of

distributed mobile agents. The agent platform can be distributed across machines with varying operating systems and the configuration can be controlled via a remote GUI. The configuration can be even changed at run-time by moving agents from one machine to another one, as and when required. Adding to this WADE provides support for the execution of tasks defined according to a workflow metaphor.

The agents when need to communicate when residing on same node are being carried out using shared memory concept as it proves to outweigh other techniques like pipes and message queues. However for implementing communication between different nodes extensible markup language (XML) is used and carried out through agent management system (AMS) of JADE framework.

A multi agent programming approach is being used to develop the prototype system. In the first step the various cooperating agents are created and registered in a global file. Each of agents are assigned with a unique identifier and copy of the global file is replicated in each of the nodes. The second step involves setting the behavior and parameters of each of the agents. This step is followed by defining the methods to perform the tasks of each agent. This system makes use of various flags to check the status of the agents and availability of visiting agents. The usage of flags to control the activity of various agents helps in maintaining battery power in the nodes.

One of the significant steps in the implementation process is development of attack libraries. The attack libraries which are compatible with JADE are created for basic MANET attacks. These are further refined through learning and adaptive algorithms to develop complex attack rules. The overall logic of the system is implemented in JADE and the various key functional modules integrated through API calls.

5. Relative Merits

The relative merits of the proposed approach can be summarized as follows. The learning module with in-built fuzzy inference engine uses associative mapping rules and decision tree algorithms to detect new attack patterns. These are eventually fed into rule base of individual hosts. Thus false positives are decreased rendering adaptability to the IDS configuration.

Another significant advantage is the use of communication agents to collect information from the host and network databases. The collected data is filtered and processed at learning module to identify attack patterns. Hence the nodes are relieved off the processing burden, thereby saving power and other resources.

The use of Java programmed mobile agents to perform the intrusion detection tasks make the scheme effective. The roaming agents are sent by learning module whenever new rules need to be updated at local node rule bases. The mobile agents are tamper evident as the agents are programmed as read only and information can be written into the agent in append mode. Also every roaming agent bears a timestamp and hash value of the data encrypted with a key known only to the learning module. When a roaming agent returns back to the learning module the encrypted timestamp and hash value of data can be decrypted using the secret key and further, the hash of the data can be recalculated and rechecked for any possible data modification. Thus any corruption of data can be detected and this makes the scheme self-secure and tamper evident.

The hybrid scheme of rule-base and behavior based approach improves the detection rate. Any selfish or malicious node can be filtered out since the proposed scheme utilizes collective monitoring and analysis at the test bed. Thus false rules are not getting added to the rule base and the IDS scheme is protected from corruption of rule base.

6. Conclusion

Through this paper, I have brought out a distributed intrusion detection scheme for MANETs which is based on the programmable mobile agents. The distinguishing feature of this approach is that it make use of the light weight mobile agents which are very well suited for the resource constrained mobile nodes. Another remarkable highlight of the proposed scheme is the division of intrusion detection tasks among both the network and host monitoring

agent and use of learning module which injects new attack rules to the system. Both these concepts address the inherent challenges faced by IDS installation in MANETs. Moreover the mobile agents are made tamper evident to detect any potential attempt to corrupt the attack related data being carried by them. The experimental setup implemented using WADE framework will bring concrete results to show the effectiveness of the proposed system.

References

1. Y. Zhang and W. Lee. Intrusion Detection in Wireless Ad-hoc Networks. In: Proceedings of the 6th Annual International Conference on Mobile Computing and Networking Mobi Com 2000. p 275-83.
2. B Smith. An examination of an Intrusion Detection Architecture for Wireless Ad-Hoc Networks. In: Proceedings of 5th National Colloquium for Information System 2001.
3. Jansen et al. Applying mobile agents to Intrusion detection and response. NIST Interim Report No-6416. San Francisco: National Institute of Standards and Technology Computer Security Division; 1999.
4. Crossbie. M., Spafford.E. Defending a Computer System Using Autonomous Agents. In: Proceedings of the 18th National Information Systems Security Conference October 1995.
5. Tripathi, A.R. A security Architecture for Mobile Agents in Ajanta. In: Proceedings of the 20th International Conference on Distributed Computing Systems 2000; Washington DC; 2000. p 402-09.
6. P. Albers, et al. Security in Ad-hoc Networks, a general intrusion detection architecture enhancing trust based approaches. In: Proceedings of First International Workshop on Wireless Information Systems: 2002 April 3-6; Cicidad Real, Spain.
7. O.Kachirski and R.Guha. Intrusion Detection Using Mobile agents in Wireless Ad-hoc Networks. In: Proceedings IEEE Workshop on Knowledge Media Networking: 2002 July 10-12; CRL Kyoto, Japan. p 153-58.
8. Monika Darji and Bhushan Trivedi. Secure Leader Election Algorithm Optimized for Power saving using Mobile Agents for Intrusion detection in MANET. In: Sabu.M. Thampi.et al, Authors. SNDS 2012. Proceedings of the recent trends in computer networks and distributed system security; 2012 Oct 11-12, Trivandrum, India; 2012. p 54-63.
9. Yinghua Guo, Steven Gordon. Ranger, a Novel Intrusion Detection System Architecture for Mobile Ad hoc Networks. In: Proceedings of TENCON 2005 ; Melbourne. p 1-6.