An Agent Based Security Framework for Emering Networks

Javed Ahmed[†], **and Shiraz Latif**[††], **Sangeeta Lalchand**[†††], **Mazhar Manzoor**[††††]

National University FAST Karachi Pakistan, Mehran University Jamshoro Pakistan

Summary

Mobile ad-hoc network has gained enormous amount of attention during last few years due to its wider application area from conventional military purposes to emergency response service. MANETs throws up new requirements and problems due to flexibility and dynamic nature of these networks. The challenges faced in the Ad-hoc environment are mostly due to the resource poorness of these networks. These types of networks operate in the absence of any fixed infrastructure; therefore solutions for conventional networks are usually not sufficient to provide efficient operations in ad-hoc environment. The wireless nature of communication and lack of any security infrastructure raise several security problems. In this paper we propose an agent based framework for MANET security. The proposed approach is scalable and has a minor dependence on central node. Mobility feature of software agents address the issues of dynamic topology and unpredictable traffic patterns.

Key words:

Ad-hoc networks, Intrusion Detection Systems, Mobile Agents, Cryptography

1. Introduction

Mobile ad-hoc network is a network of a number of mobile routers and associated hosts, connected by wireless links [1]. These networks are characterized as infrastructure less, mobile, autonomous, multi-hopped, self-organized and self-administered, having dynamic topology and unpredictable traffic patterns. In the perspective of network architecture, ad-hoc networks are classified as either flat or multi-layered. Flat ad-hoc networks are peer to peer in nature, whereas in multi-layered architecture, one or more heads are dynamically elected, that are responsible for co-ordination among the nodes. Due to the lack of an underlying infrastructure, basic functionalities, such as routing, configuration of the hosts or security management cannot rely on predefined or centralized entities to operate, and must be carried out in a distributed manner. Security requirements in wireless networks are nonetheless identical to those in wired networks. Existing research conducted to providing security in mobile ad-hoc networks can be grouped into three major categories: 1) providing security infrastructure like PKI, 2) Secure routing and 3) Intrusion Detection Systems [2]. As far as secure routing is concerned, most of routing protocols proposed for ad hoc networks have not enough mechanisms to defend against malicious attacks [3, 4, 5]. As a result, these protocols are exposed to variety of attacks such as message replay, false routes, network partitioning etc. One of the ways to protect routing information is to use cryptographic approaches such as digital signature. A highly secure and highly available key management service based on Threshold Cryptography technique is presented by [3].

Intrusion Detection system (IDS) is another way to provide security and privacy in MANET. Intrusion detection can be defined as a process of monitoring activities in a system by capturing user’s activities called audit, analyzing the audit and inferring from this profile if there are any security violations [5]. The user’s activity can be captured at the hosts (host based IDS) or at the edge/ gateway of the network (network based IDS) [5, 6, 7]. IDS can be classified into two basic types based on the type of data being captured; (i) Anomaly Detection Model; (ii) Misuse Detection Model [7, 6]; the earlier model analyze node activities to conclude about abnormal behavior of the node. The later model compares node activities against a database of signatures for drawing its conclusion about the node behavior. Network based IDS systems are generally not possible for MANET because it is generally not possible to capture audit data at the edge of the network [6].

This paper focuses on security concern in MANETs. Rest of the paper is organized as follows: section II presents literature review. In section III, we see why mobile agents are adapted for intrusion detection in the decentralized nature of MANETs. Section IV proposes agent based security framework for MANETS. Finally, we conclude and present our future directions.

2. LITERATURE REVIEW

Mobile Ad-hoc network is active research area. A great deal of research is being conducted to address various issues of MANETs. These issues include Routing, MAC Layer issues, Power Management and Security [8, 9, 10]. Security is one of the most important issues in MANETs.

Manuscript received June 5, 2010
Manuscript revised June 20, 2010

The nodes in MANETs are highly dependent on one another and required to trust each other for smooth network operations. But, MANET is often deployed in highly hostile environment, and it is always susceptible to a range of security risks, ranging from passive eavesdropping to active interference. So, providing security and trust management capabilities to MANETs is one the most crucial issue.

In literature, a number of approaches to providing security and trust management using IDS have been proposed. A good survey of common IDS techniques has been provided in [5]. The general mechanism to provide IDS is to run a frame-work/daemon on every host. These daemons will capture the audit data and can also distribute this information to peering nodes or some elected heads [5].

The IDS model based on mobile agents has proposed by [11]. The basic idea is the selection of a fixed centralized entity. The role of this central entity is limited to launching mobile agents at the arrival of new node in to the network. The launched agents will perform initial security measures on the newly arrived node and then distributing network topological information to the new node. According to [12], and [5], by employing mobile agents, various benefits like 'Threshold Cryptography', up-to-date topological and behavioral information; fault tolerance and scalability can be achieved.

Another framework based on mobile agents has been proposed by [13]. This IDS solution is conceived by forming an analogy of MANET with human body. The IDS works like Human Immune System and similar to antibodies of human body, agents running on every host watches out any new arrival host for possible intrusion. In case of any intruder been detected, new agents are launched to isolate the intruder from the network.

3. AGENTS SUITABILITY FOR AD-HOC ENVIRONMENT

Software agents consist of program code and state [14]. Agents are used to perform tasks on behalf of a user with some degree of autonomy. A software agent's goal may require some degree of intelligence, allowing it to react to its environment, make plans to achieve its goal, maximize its utility, and/or modify its behavior over time. Software agents may use mobility to travel to sources of data and remotely execute their tasks, resulting in a natural distribution of work and reduced communication overhead [15]. An agent is lightweight programs that accomplish their essential tasks with minimal code. It is dynamically updatable and upgradeable, smaller, simpler, and faster to transport. An agent will only carry the primary features to make it lightweight; after it arrives the destination system, it will be upgraded and updated as necessary for the situation. Using this design objective, the system will be able to be deployed in resource constrained environments to monitor communication activities of nodes. Mobile agents do not require network connectivity with remote services to interact with them due to this feature they are perfect suitable for ad-hoc environment with high mobility. Results in the form of data do not necessarily return to the user using the same communication trajectory, this also support unpredictable moving patterns. So mobile agents have many advantages for ad-hoc environment and they solve critical problems encountered in highly mobile and bandwidth limited wireless mobile ad-hoc networks.

4. AGENT BASED SECURITY MODEL

We are proposing an agent based framework for multi layered ad-hoc environments. This framework is based on two modules (i) Local Intrusion detection system (LIDS); (ii) Global intrusion detection system (GIDS). A LIDS is running on every host in the network, whereas GIDS is running only on manager node.

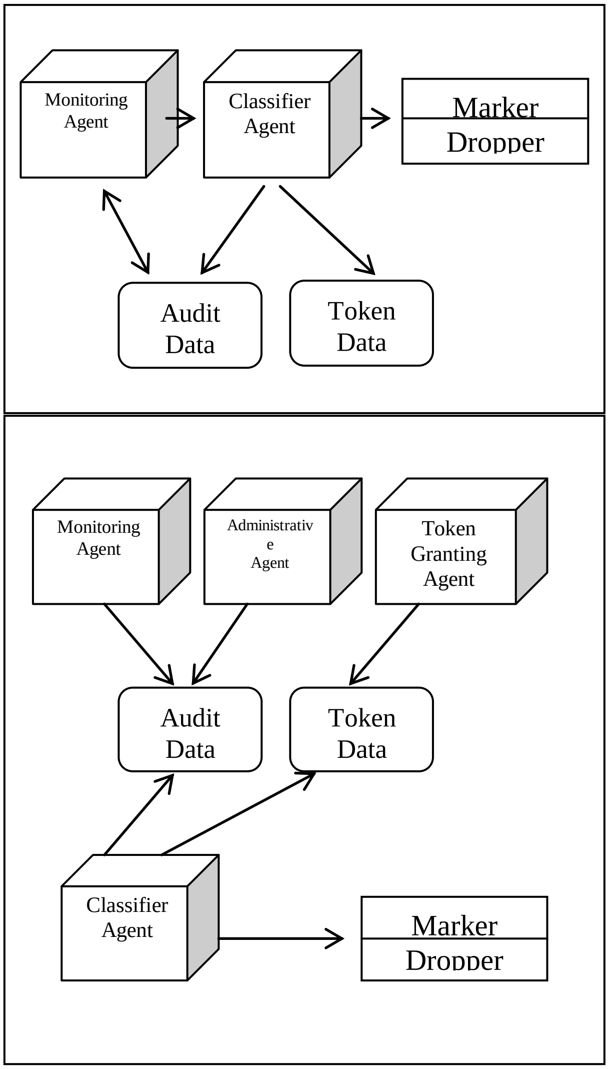
One of the most important issues is to decide manager node? In order to resolve this issue one of the existing node will be elected as manager node by the means of election algorithm. There are numbers of election algorithms [17] that can be used for this purpose. All of these algorithms require some priority values to be used for election purposes. In our case, we have eliminated very young and old nodes (based on their average age) from being candidate for manager. Young nodes are eliminated because we don't have accurate information about their profile rating. Old nodes are eliminated because they are about to leave the network and then we will require another election.

After discovery of manager node, it will first of all perform initial security checks and launch GIDS and LIDS. These modules will provide security services to all nodes joining the network.

The manager will be running GIDS modules which provide basic services such as issuing a token and isolating a malicious node. The GIDS is based on four agents (i) Monitoring Agent; (ii) Administrative Agent; (iii) Token Granting Agent; (iv) Classifier Agent. Every node on network will be running a monitoring agent that will record the behavior of other nodes in the audit data. The monitoring agent can also trigger the administrative agent to isolate an intruder from the network. Token granting agent issues token to newly arriving nodes. The token will be used for the unique identification and authentication of the nodes into the network. When any node wants to communicate with other node, it will have to first show its token to the communicating node. The communicating node can verify the integrity of the node by analyzing its token data. Hence, the reputation of the nodes in the network can be determined by token and audit data. If the reputation of any node is decreased from certain threshold value then monitoring agent triggers administrative agent to isolate the node from the network. Every node on the network will be maintaining profiles of every other node in the network and recoding this information in an audit database. The profile will simply be a list of attributes reflecting the actions / behaviors of a node. These attributes of a node can be the size of the packet, the type of the data, and recipient to which message is mostly sent; the intermediate hops through which a message is received etc. These attributes can be used to profile rating.

The LIDS will be based on two agents (i) Monitoring Agent; (ii) Classifier Agent. LIDS assume that node activities are observable, which means that a node initiated activities get logged somewhere into the system logs. Intrusion detection system has an easy access to these logs (audit data). All nodes in the network maintain the profiles of all other nodes on the basis of audit data and token data. The profile information is updated temporally, which calculate reputation of the node by involving all other nodes. Each node rates all other nodes on basis of activities initiated by the nodes. If any node is involved in malicious activities and this is analyzed by monitoring agent on the basis of audit data and token data then monitoring agent trigger the classifier agent to mark the packets of the node. Marker with packets of doubtful node is used to alert the other nodes on network. All other nodes in network either support or oppose observation of the node appended marker with packet. If support reach to certain threshold then GIDS takes necessary action to isolate node from network as mentioned in above discussion of GIDS.

All nodes will be sensing the presence of every other node on the network by sending periodic heart beat messages to each other. After the crash of any node on the network GIDS will trigger ‘administrative agent’ to clear the information related to that node. In case of failure of manger node, an election algorithm will be initiated and a new node will be elected as manager. Note that failure of manager will not result in the loss of any cryptographic information because token database containing public keys of all the other nodes will be available on all the nodes including the newly elected manger. Hence our approach has minor dependency on manager node.



In this paper we have proposed a security model for MANETs. The proposed approach is scalable and has a minor dependence on central node. The theme of idea comes from those countries of world which are popular federations. These federations provide basic services to states and the states are nearly autonomous. In our case, GIDS act as a federation and provide basic services of issuing tokens and isolating malicious node on recommendation of all other nodes. LIDS acts as autonomous state and free to take necessary action for securing it. Upon crash of a central node, a new node can be elected as manager using election algorithm. By employing mobile agents running on each node this security model will work efficiently to prevent the malicious nodes from harming the network.

6. References

[1] "IETF Mobile Adhoc Networks (MANET) Charter", http://www.ietf.org/html.charters/manet-charter.html, last accessed on 18th June, 08

[2] Shuyao Yu, Youkun Zhang, Chuck Song, Kai Chen, "A security architecture for Mobile Ad Hoc Networks", APAN Network Research Workshop, 2004.

[3] Lidong Zhou, Zygmunt J. Haas, "Securing Ad Hoc Networks", IEEE Network Magazine, 13(6):24–30,November/December 1999

[4] Azzedine Boukerche et al., "Performance Evaluation of Routing Protocols for Ad hoc Wireless Networks", Mobile Networks and Applications 9, 333–342, 2004, 2004 Kluwer Academic Publishers, Manufactured in The Netherland

[5] Y. Xiao, X. Shen, and D.Z. Du, "A Survey on Intrusion Detection in Mobile AdHoc Networks", Chapter 7, Wireless/Mobile Network Security, pp. 170 – 196, 2006

[6] Farooq Anjum, Dhanant Subhadrabandhu and Saswati Sarkar, "Signature based Intrusion Detection for Wireless Ad-Hoc Networks: A Comparative study of various routing protocols", Vehicular Technology Conference, 2003. VTC 2003 Fall. 2003 IEEE 58th

[7] Y Zhang, W Lee, & Y Huang, "Intrusion Detection in Wireless Ad-Hoc Networks", Mobile Networks and Applications, 2003.

[8] Samba Sesay, Zongkai Yang and Jianhua He, "A Survey on Mobile Ad Hoc Wireless Network", Information Technology Journal 3 (2): 168-175, 2004, ISSN 16826027, © 2004 Asian Network for Scientific Information.

[9] Quan Le T., "Mobile Ad Hoc Networks towards Internet and Next Generation of Internet", PhD Dissertation I, Department of Telecooperation, JKU, Linz AUSTRIA, Dec.2004

[10] E.M. Royer and C.K. Toh, "A review of current routing protocols for ad-hoc mobile wireless networks" IEEE Personal Commun., 1999

[11] Roshan A. Shaikh and Zubair A. Shaikh, "A Security Architecture for Multihop Mobile Ad hoc Networks with Mobile Agents", INMIC, 2005

[12] Toh, P. Mahonen, M. Uusitalo, "Standardization Efforts and Future Research Issues for Wireless Sensors and Mobile Ad Hoc Networks", IEICE Transactions on Communications, Vol. E88B, No. 9, 2005

[13] Yj Ping, Yao Yan, Hou Yafei, Zhong Yiping, Zhang Shiyong, "Securing Ad-hoc Networks through Mobile Agent", Proceedings of the 3rd international conference on Information security, 2004

[14] Franklin, S., and Graesser, A., Is It an Agent or Just a Program? Taxonomy for Autonomous Agents. Proceedings of the Third International Workshop on Agent Theories, Architectures, and Languages. New York: Springer-Verlag.

[15] Ghulam Ali, Zubair A. Shaikh, Noor A Shaikh, The Design and Implementation of an Agent Framework to Support Distributed Problem Solving, published in Conference Proceedings, 25-27 September 2007, Athens, Greece, and accepted for Springer-Verlag publications to be released in November 2007.

[16] Pradeep K Sinha, "Distributed Operating Systems: Concepts and Design", 2002.

[†]**Javed Ahmed** is a PhD fellow in National University of Computer and Emerging Sciences Karachi. He received the B.Sc. and M.Sc from Sind University Jamshoro Pakistan in 2001 and 2002 respectively, completed his M.S. degrees in Computer Science from National University of Computer and Emerging Sciences FAST Karachi Pakistan. Currently he is working as a visiting researcher in University of Paderborn Germany on Ph.D Exchange Scholarhip (for short research).

[††]**Shiraz Latif** is a PhD student in Mehran University of Engineering and Technology Jamshoro Pakistan. He did his B.E. from IIEE-NED university of Engineering and Technology Karachi in 2001. After that he did his first Masters in Computer Science from NU-FAST and second Masters from Usman Institute of Technology- Hamdard University Karachi Pakistan.

[†††] **Sangeeta Lalchand**

[††††]**Mazhar Manzoor**