ISSN:0975-9646

Yogendra Kumar Jain et al, / (IJCSIT) International Journal of Computer Science and Information Technologies, Vol. 3 (4) , 2012,4798-4805

Secure Mobile Agent Based IDS for MANET

Yogendra Kumar Jain, Rajesh Kumar Ahirwar

Computer Science & Engineering Department,
Samrat Ashok Technological Institute, Vidisha, (M.P.), India

Abstract- Mobile Agents are used to share the utility to collect information from various nodes. We have given consideration to the security of Mobile Agents. This paper proposes an algorithm which is based on dummy agent. In this paper we are proposing a secured mechanism to manage the security of the mobile agents being transferred to the various nodes. For security of the mobile agents, we are sending a dummy agent to the wireless node which will first check if the node is malicious or not. If node is not malicious then the dummy agent acknowledges to the source station and source station node transfers the actual mobile agent to the wireless node. In case the mobile agent suffers some intrusions at the wireless node then to cope up with that another supervisor agent is also transferred along with the mobile agent. This supervisory agent informs to the source station about the intrusions or kills the mobile agent at wireless node before intruder infects to it. This will cause to have high security on the mobile agent. We will be encrypting the data on mobile agents before transferring to other nodes.

Keywords- IDS, Supervisory agent, Mobile Agents, Dummy Agents,MANET.

1.INTRODUCTION

Mobile ad hoc networks (MANET) are wireless networks in which the mobile nodes trade information without the help of any predefined network infrastructure. In such networks, also called unstructured networks, the nodes work together to provide the basic network services. For example, in the case of routing, the lack of a network infrastructure implies that the service is usually provided in a peer-to-peer manner and that all the nodes of the network need to act as collaborating routers. Nodes in a MANET may, at any time, disappear from, appear into or move within the network. The resulting dynamic nature of the network topology, along with the unreliability of the wireless links, require for the configuration of MANET services to be highly adaptable. Moreover, the availability of an individual node cannot be assured and therefore, services cannot rely on a central entity and must be provided in a distributed and adaptive manner. Security services are not an exception to this general rule and many traditional approaches are usually unsuitable for MANET [1].In this paper, we are interested in designing secured mobile agent based IDS for MANET. Our first objective is to provide mechanism to detect intrusions on MANET using mobile agents and second is to provide the security of the mobile agents working in this scenario. In our design, we use the mobility and autonomy associated with mobile agents to provide an efficient and flexible solution to poor connectivity and limited bandwidth in MANET context.

Our first objective is achieved through the application of the various rules incorporated in the mobile agents. Mobile agents will work as a carrier for IDS to move to a particular wireless node and collect information from the node. This information is transferred to the base station, which will make the decisions related with the attacks on the concerned nodes. Second objective of our proposed mechanism is achieved by sending a dummy agent on the wireless node to detect if the node is malicious. If the node is safe then we are allowing transferring actual mobile agent, which is also secured. Transfer of information from wireless node to base station is also encrypted; therefore information security is involved in the infrastructure devices such as intermediate routers etc. as well.

2. BACKGROUND

MOBILE AGENT BASED IDS

Intrusion detection is based in collection and analysis of system and network audit data. Upon detection, intrusions should be reported to security management. Also, an automatic response, aiming to eliminate the causes and/or effects of the intrusion, may be triggered. Given the lack of centralization, the mobility of the nodes and the wireless nature of link connections in the MANET environment, some (if not all) tasks required for the intrusion detection process described above should be executed in a distributed and cooperative manner [4]. In our design, an IDS is placed within the mobile agent to be sent on each node of the MANET. The IDS communicate using a mechanism that takes into account the restrictions resulting from the MANET context; e.g. limited bandwidth or poor connectivity. Such architecture has already been identified in [4] as a basic requirement to IDS for the MANET environment. To provide flexible and autonomous means of interaction between the node and base station, we have proposed to use mobile agents[5 &10].If an IDS fails to cooperate during some period of time (e.g. it has moved away, cracked or is compromised by some intruder), the intrusion detection service must not degrade. Redundancies in the MANET compensate for the nodes that are not cooperating in the detection processes as it is possible for more than one node to track and detect the same attack. Mobiles agents are an alternative to the client-server distribution model [10]. The use of mobile agents, opposed to traditional approaches where data are transported towards the computation location, allows the code to move toward the data. Carefully designed agents can reduce the amount of data exchanged through the

network, while providing a flexible way of distribution. Also, a node dispatching an agent doesn't have to wait for it to return to resume the processing and an agent can be dispatched and even destroyed by other nodes, without having to move back to the originator node. In our design, cooperation may be done in different stages of intrusion detection. During data collection, nodes exchange information about events to build the intrusion evidence.

In detection algorithm execution, IDS exchange information about the current state of the structure implementing the detection algorithm. Finally, alert correlation is also possible, when a node uses alerts from others to enforce the evidences of the suspicious activities detected locally on the wireless node. In any case, cooperation is executed by means of a mobile agent that roams from one system to another. Mobile agents can also provide a first element of response to the dynamic nature of MANET topology and membership. Indeed, when a node joins the network, it does so with a running IDS and a mobile agent platform. Keeping the collaboration within a restricted number of nodes relates to bandwidth usage and scalability requirements. The rationale in executing some of the detection tasks only in the local neighbourhood is double justified on the very nature of the MANET. A MANET node naturally has to collect and maintain information about its neighbours. Moreover, any information going to or coming from a MANET node should be routed through one of its neighbours, when it may be promiscuously monitored, given the broadcast nature of the wireless links [1]. Thus, neighbours from a node being target by an attack are naturally eligible as primary sources of information about the status of the node suffering the effects of the attack. Neighbour nodes are also eligible as collaborating peers to uncover information related to the intrusion that is lacking locally.

MECHANISM OF IDS

Data can be collected from different audit sources, which can be a network packet capture interface (network level), a log system (host level) or a MIB (network, host and/or application levels). The data collected directly from the audit source is hereafter referred as raw data. These data are usually raw and has poor semantics. Also, raw data is available in a format that depends on the data source. Some pre-processing is applied to raw data, translating it into semantically richer information used by the detection algorithm, which are called events. This transformation on raw data is referred as event abstraction. Event abstraction can use many different techniques, such as pattern matching [6], data-mining [12] or statistical correlation [4]. We have decomposed sensor in two modules: Event Abstractor and Data Collector.

These modules separate the data retrieving and the event abstraction features in two different entities. The idea is to enable multiple implementations for the Data Collector module, which may operate simultaneously collecting data from different sources, while enabling the event abstraction process to have abstraction rules that use information originated from multiple sources. Implementations of the Event Abstractor module with different abstraction principles are also possible.

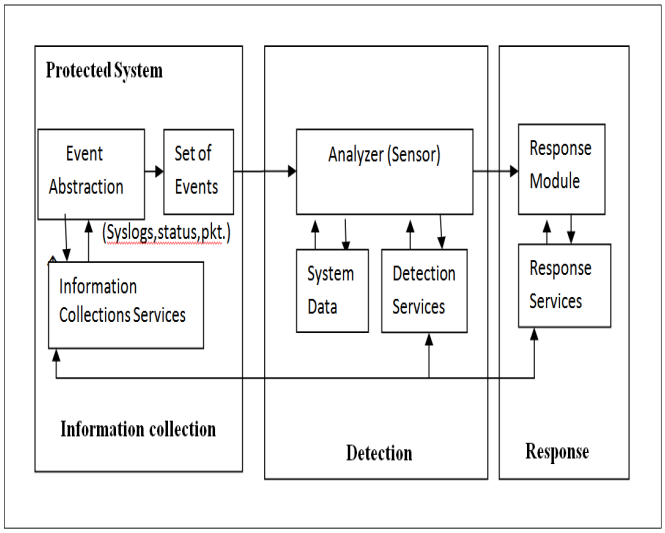


Figure: 1 IDS component

Fig.1 describes the Analyser processes events according to some defined detection strategy. At least two detection methodologies are currently in discussion: misuse and anomaly detection [11]. It seems to us that these methodologies are complementary. It is our goal to have a hybrid (misuse and anomaly) intrusion detection strategy. In our architecture, each detection algorithm implementation is encapsulated in an IDS Kernel module, and it is possible to have multiples instances of such module, each one with specific detection algorithms. A concise representation of the current status of the detection algorithm is represented in a detection state message. Such information can relate to the state of the detection of a specific attack, in misuse detection, or to the state of the behaviour model shown in fig.2, in anomaly detection. The Manager relates to alert management and intrusion response tasks. The Alert Manager module is designed to accomplish with the alert management, performing operations such as alert interpretation, false positive elimination and alert correlation.

Prevention

Simulation

Intrusion Monitoring

Analysis

Intrusion Detection

Notification

Response

Figure: 1.2 Intrusion Detection System Activities

In most distributed IDS architectures, distribution is restricted to data collection. In IDS for ad hoc networks, this is

mandatory, as remote collection of important volumes of data is prohibitive due to limited bandwidth. Besides of local data collection, we also want to make a complete distribution of IDS tasks, enabling execution of the detection algorithm and alert management to be equally realized in a distributed manner. In our design, data collection and event abstraction are always kept local. Exchanged data are only concise information (events) resulted from local pre-processing of raw data. Cooperation in execution of the detection algorithm is done by exchange of detection state messages, while alert correlation relates to the exchange of alert messages. We propose that distribution and cooperation are accomplished by means of mobile agents, which are created, dispatched and managed through the Mobile Agent Framework. All high level messages to be dispatched to or received from other nodes are sent to Distribution Manager. This module decides where the messages should be delivered and processed.

MOBILE AGENTS

Mobile agents are mobile autonomous processes operate on behalf of users in a distributed computing environment. The autonomous agent concept has been proposed for a variety of applications on large, heterogeneous, distributed systems (e.g., the Internet) [22]. These applications include a specialized search of a middleware services such as an active mail system, large free-text database [24], electronic malls for shopping, and updated networking devices. Mobile agent systems have many advantages over traditional distributed computing environments. They use less network bandwidth, increase asynchrony among clients and servers, dynamically update server interfaces and introduce concurrency [23].

Due to the problems with security of Mobile agents have limited their popularity. Mobile agents are composed of code, data, and state. Agents migrate from one host to another taking the code, data and state with them. The state information allows the agent to continue its execution from the point where it left in the previous host. For example, a mobile agent could be migrated from the home platform with the task of buying an airplane ticket for its owner. The agent would visit all the known hosts of airline companies, one after another, to search for the most reasonably priced ticket, and then purchase one for its owner. Each time the agent moves to the next host, it summarizes the current state, execution pointer on the current state, etc., so that it can start searching for reasonable tickets on the next host. The state of the agent will contain a set of possible tickets to be considered for purchase. When the agent has finished its search, it may return to the host where it found the cheapest or best ticket and purchase it.

While agents roam around the Internet, they are exposed to many threats and may also be a source of threat to others. Sander and Scudding present two types of security problems that must be solved [25]. The first is host protection against malicious agents. The second is agent protection against malicious hosts. Many techniques have been developed for the first kind of problem, such as password protections, access control, and sand boxes, but the second problem seems to be difficult to solve. It is generally believed that the execution environment (host) has full control over executing programs; thus, protecting a mobile agent from malicious hosts is difficult to achieve unless some tamper-proof hardware is used.

3.LITRATURE SURVEY

1. **D. Barman Roy1 and R. Chaki** proposed a new Intrusion Detection System (IDS) based on Mobile Agents. The approach uses a set of Mobile Agent (MA) that can move from one node to another node within a network. This as a whole reduces network bandwidth consumption by moving the computation for data analysis to the location of the intrusion. Besides, it has been established that the proposed method also decreases the computation overhead in each node in the network [29].

2. Panthi N.K. had proposed a scheme which not only confirms the security of data but also guarantees the uninterrupted operation of agent by utilizing a dummy agent and composite acknowledgement technique. Their simulation also shows that no agent blocked for any number of faulty nodes. Some draw back shows the increase in delay, they have not considered the security of monitoring agent, the processing time needed is also higher.

They surveyed three approaches for the problem of mobile agent protection. The three approaches are chosen because each approach is very uniquely implemented and has strengths that other approaches do not have; they choose Partial result authentication code approach because it can protect results from mobile agents. Computing with encrypted functions approaches is chosen because it tries to scramble code and data together. An obfuscated code approach is chosen because it scrambles an agent's code in such a way that no one is able to gain a complete understanding of its function [30].

3. Puttini R. and jean-Mare P. Proposed a mobile agent based IDS system in which mobile agents are transferred to wireless nodes and perform IDS operations to detect the intrusions. The work done in this paper is oriented on MIB and focused more on functionality and feasibility validation or the design [26]. They have focused only on working of IDS in distributed systems and also another future important issue is the security of the mobile agent platform [26].

4. Kumar R. and Dr. Dave M. have proposed mobile agent as a mechanism to handle the traffic problem on road. Mobile software agents can be used to provide the better QoS (Quality of Service) in vehicular ad hoc network to improve the safety application and driver comfort.

One reason is probably that such platforms have been developed with a fixed distributed environment in mind, and not considering the features that\ may be of special interest in a mobile environment (e.g., reliance against security threats, adaptation to the network technology, and service/node discovery) [31].

5. **Saidat Adebukola Onashoga** In this paper, the writer proposes a way of classifying a typical IDS and then strategically reviews the existing mobile agent-based IDSs focusing on each of the categories of the classification, for

example architecture, mode of data collection, the techniques for analysis, and the security of these intelligent codes. Their strengths and problems are stated wherever applicable. Furthermore, suggested ways of improving on current MA-IDS designs are presented in order to achieve an efficient mobile agent-based IDS for future security of distributed network.MA technology is very suitable to solve intrusion detection in a distributed environment (Chan & Wei, 2002), hence the advent of Mobile Agent based IDS (MA-IDS). MA-IDSs are also faced with some shortcomings such as:

a. High time to detection: MA solutions may not be fast enough to meet the needs of IDS.

One of the major challenging problems facing MA-IDS is improving the speed with which they can identify malicious activities.

b. Performance: though MA technology has improved greatly on detection performance, but effective detection of autonomous attacks is still very low. Also, agents are often written in scripting or interpreted languages, which are easily ported between different platforms. Their mode of execution is still very low compared to native codes (Kruegel and Toth, 2002).

c. Security: Another major problem is protecting the protector (MA-IDS) from attacks [32].

6. **Zeng-Quan Wang** have describes the function of entities in detail. The proposed model is an open system with good scalability. Agents are independent individually, while they can communicate and cooperate one another to take actions. Then the key modules are implemented in mobile agent platform-IBM Aglets and the results of experiments are discussed and analyzed quantitatively. Cooperative agents in system collaborate each other equally. We adapt the mode that does not have control centre, which avoid the matter of a single point failure [33].

4. PROPOSED ALGORITHM

The proposed mechanism also ensures following Phases shown in figure 3.I have implemented the proposed algorithm using Microsoft visual studio C#.Net. For mapping of Mobile Agents, a C# class has been created which a node every time a user clicks on the canvas. A line tool has been provided to show wired nodes, if any. A random generated Intrusion and Intrusion Detection System has been applied on each node, which causes a node to be intruded or detection of intrusion respectively. On similar lines, a malicious activity class has been designed to make a node infected. Steps in providing the secured implementation of the same are follows like as Dummy Agent, Supervisor Agent and Mobile Agent classes are used as per their requirements. Complete phases are as follows.

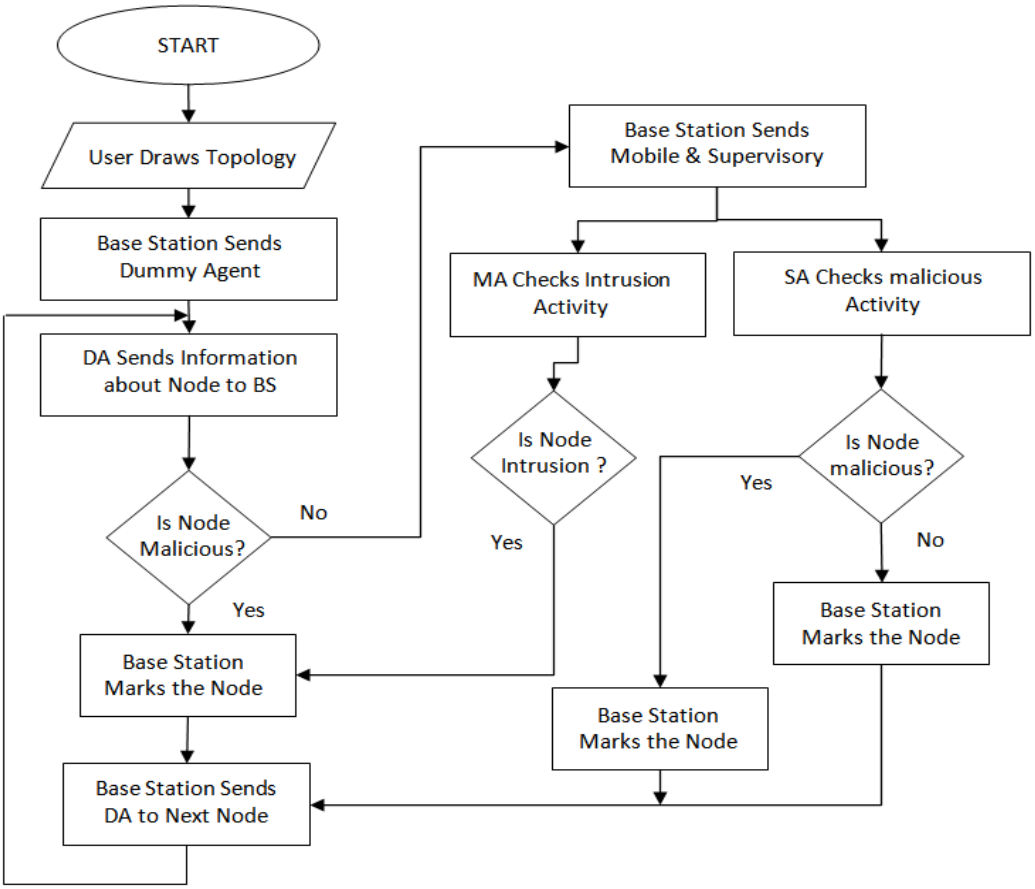


Fig.3 Flow chart of our proposed Scheme

Step 1: **Working of Dummy Agents**

1. User Draws the Network Topology using the Interface provided for which User Clicks on the Node Icon to draw Nodes and Line Icon to draw the connection between them.
2. On all individual nodes a Mal-activity Agent and various counter variables has been added for performing detection and remembering the parameters.
3. As User Clicks on Start Button a Dummy Agent is sent to all the nodes one by one, i.e. it first goes to first node and then after checking if the node is malicious or not and setting corresponding variable, it moves to next node.
4. Dummy Agent, after checking the node, informs to the base node about the node's status.
5. This information is used by the base station to generate the result data.

Step 2: **Working of Supervisory Agent**

1. User Draws the Network Topology using the Interface provided for which User Clicks on the Node.
2. On all individual nodes a Mal-activity Agent and various counter variables has been added for performing detection and remembering the parameters.
3. As User Clicks on Start Button a Dummy Agent is sent to all the nodes one by one, which informs to the base node about the node is malicious or not. If the node is not malicious base station sends a mobile agent and supervisory agent to the node.
4. Mobile agent performs its process of intrusion detection and supervisory agent checks the node status, if a timer based mal activity occurs at the node then it kills the mobile agent and sets the variable to its status as mal activity performing node.
5. Supervisory Agent informs to the base node about the malicious activity.

Step 3: **Working of Mobile Agent**

1. User Draws the Network Topology using the Interface provided for which User Clicks on the Node Icon to draw Nodes and Line Icon to draw the connection between them.
2. On all individual nodes a Mal-activity Agent and various counter variables has been added for performing detection and remembering the parameters.
3. As User Clicks on Start Button a Dummy Agent is sent to all the nodes one by one, which informs to the base node about the node is malicious or not. If the node is not malicious base station sends a mobile agent and supervisory agent to the node.
4. If Mobile Agent finds that the node has been intruded by the intrusion using the intrusion detection system it carries. If the node is intruded it informs to the base node that the node is intruded.
5. Base node uses the information to generate the data.

Step 4: Working of Encryption and Decryption

When Mobile agent is sent to the node and it detects the node's status for intrusion, It encrypts the information before sending it to base station, so that any other intermediate node must not be able to misuse the information. Base node decrypts the data related with the intrusion to generate the required data.

5. SIMULATION TOOL

We are implementing the above system using Microsoft Visual Studio .Net (ver. 2010) with C# programming Language and for Mobile Agents. The system will have two agents implemented, working on a base station. From the base station, dummy agents will be transferred to the nodes and on positive acknowledgement ;(if node safe) than actual mobile agents will be transferred to the wireless nodes. For simulation purposes a multithreading environment is created to work for multiple agents processing and C# programming is going to be used. for communication purposes. For implementation of IDS we are generating a detection system and dummy attacks as well.

6. RESULTS AND ANALYSIS

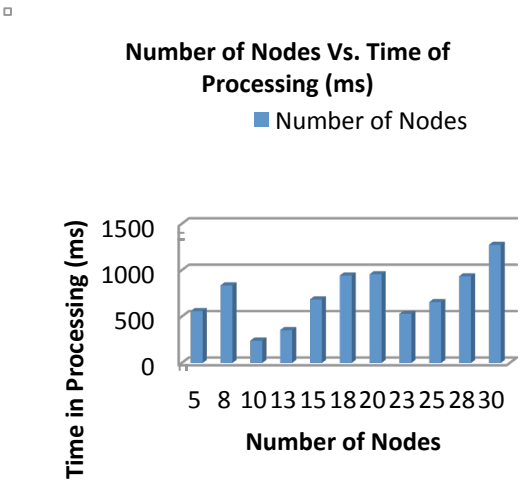
In our experimental results shows the proposed algorithm is expected to perform better in all situations as: The algorithm proposed is used to study the behaviour of mobile agents. This study is based on important Internet applications where they are believed to have better performance. Following measures has been applied to maintain the security of the mobile agents:

1. An Encryption & Decryption Mechanism has been applied to keep the data related with the intrusions, so that any intermediate nodes must not infect/steal the details.
2. A Dummy Agent is sent before the actual Mobile Agent, so that if the node infection can be detected and any data loss can be prevented.
3. A Mobile Agent itself carries a Intrusion Detection System utility to check whether the visited node(s) have any intrusions, if so that is informed to the base station.
4. A supervisory Agent is also sent along with the Mobile Agent to avoid any hidden and sleeping infections which are timed cannot infect the Mobile Agent.

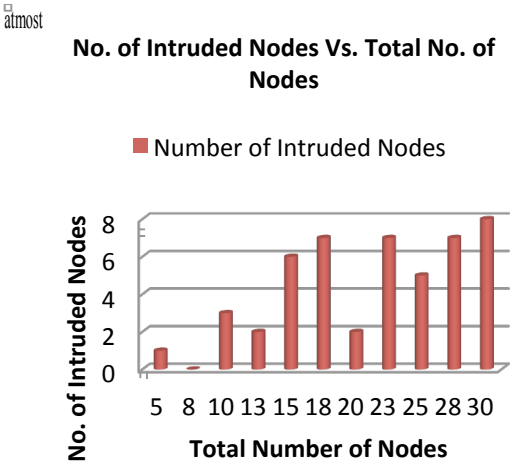
From the simulation performed following data table1 has been generated which shows the various topologies applied to test the simulation for accuracy and security

SNO	NUMBER OF NODES	CORRECT NODES	MALICIOUS NODES	DUMMY AGENT DETECTED MALICIOUS NODES	SERVICE AGENT DETECTED MALICIOUS NODES	MOBILE AGENT DETECTED INTRUDED NODES	TIME TAKEN
1	5	3	1	0	1	1	558
2	8	6	2	1	1	0	835
3	10	4	3	0	3	3	240
4	13	9	2	1	1	2	353
5	15	7	2	0	2	6	684
6	18	7	4	1	3	7	942
7	20	12	6	3	3	2	955
8	23	11	5	0	5	7	529
9	25	9	11	0	11	5	655
10	28	10	11	0	11	7	933
11	30	12	10	2	8	8	1272

Data Table 1



Number of Nodes vs. Time Taken (ms) in Secure Mobile Agents Scheme



Number of intruded Nodes vs. Total Number of nodes in Secure Mobile Agents Scheme

1. *Simulation Result for Suspicious Nodes*

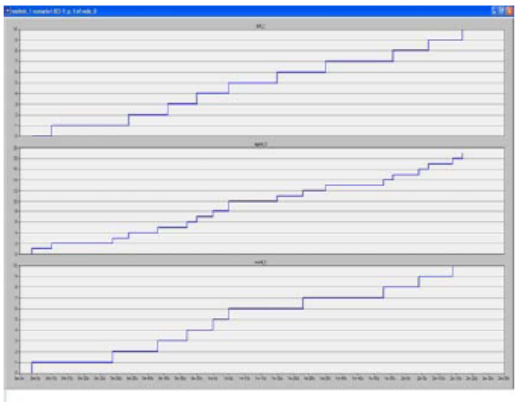


Figure 2: Simulation result for 12 nodes where 1 node is suspicious (total simulation time 300 seconds).

B. Simulation Result for Faulty Nodes

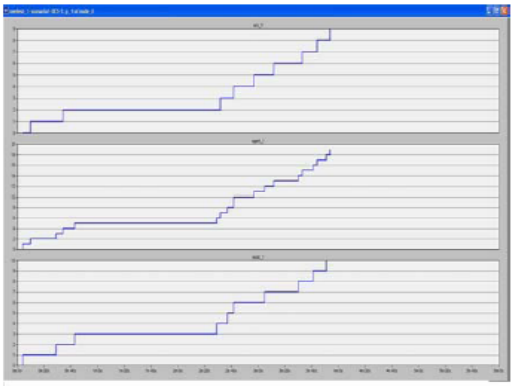


Figure 4: Simulation result for 12 nodes where 1 node is faulty (total simulation time 6.5 minutes).

I have tried running the simulation with different number of nodes and collected the information related with infected nodes and intruded nodes along with the nodes which do not have any problems. Time for running the simulation has been calculated to show that the time required to run the simulation for various topologies is not affected very much due to application of security techniques. From the above data following graphs have been plotted to shown in fig.4 the pattern of time taken in processing with varied number of nodes in the topology. The other graph plots the number of infected nodes vs. Total number of nodes applied in the topologies. The graphs are excellent and quick visualization of the processing time pattern and count of infected nodes shown in fig. 5 System. In our proposed work benefits are as follows.

1) Time elapsed in our simulation is less than the time taken in existing simulations.
2) Mobile Agent is sent with IDS for providing more security.
3) Processing of Dummy Agent is clearly defined and detection process for dummy agents' status has been added.
4) Supervisory Agent also checks if any delayed mal activity occurs at the agent.

Comparison between the existing work and Results of the proposed Algorithm: following chart shows the time taken in processing of 12 nodes for suspicious activities and Faulty Nodes

From the graphs 2 & 4 it is clear that the performance has been improved up to a great extent in my work i.e. time taken in processing is approximately 5 minutes and 6.5 minutes respectively, in contrast of 684 ms in my work for similar conditions.

In MANET, dynamic behaviour of the wireless nodes imposes many new challenges along with the count availability of nodes and bandwidth usage. Security of the nodes is also an important aspect. Application of IDS on such a system is basic need and will help stabilize the system. We have proposed an algorithm to implement secured IDS using Mobile Agents and will be able to apply the great security in the system.

We are implementing the system with utmost care to reduce the bandwidth usage and get the maximum security. Successfully implementation of such a system can reduce the network threats in MANET.

The protection of mobile agent against malicious host and very high chances of successful completion of task and depends only on bandwidth of system and time out limit of agent. It is capable of sustaining the malicious activities being generated by any host at any time because the actual data is encrypted and we can further enhance it by making agent to be self destroying in case it finds any malicious activities. The upstream node can recognize the malicious activities at downstream nodes by either receiving a negative acknowledgement by the monitoring agent or after a fixed time interval during which it has not received the acknowledgement from the monitoring agent.

7. CONCLUSION

The work done by the Panthi has not provided the security for the monitoring agent and their simulation time is also more. They also send the monitoring agent and dummy agent simultaneously so in case both agents gets tampered by the mal activities then the whole process is repeated again by the mobile agent which causes flooding in network. Our proposed approach uses a dummy agent and supervised agent..The dummy agent checks for the mal-activity and the supervised agent checks for the intrusion at the node. In case the dummy agent gets tampered the supervised agent will acknowledge the base station otherwise mobile agent is transferred to the destination. From the results it is concluded that our approach is more secure and taking less time as compared to previous work done on the mobile agent.

8. FUTURE WORKS

Our work can be further improved in future by including detection of more attacks and maintaining a database of intruded nodes on the base station, which can be dynamically updated to include the corrected and intruded nodes in future. Further improvements include utilization of specialized inter-agent communication frameworks. This modification would also provide a better framework for information sharing between agents and interoperability of various intrusion detection systems. Our system still contains several single points of failure. Elimination of these functionally critical failure points is a major challenge. Making them mobile as the rest of the components could be a way of solving the problem. However, it is not clear how this affect the performance of the overall system. There are many other applications where mobile agent technology seems to be promising and can be further studied. These include but are not limited to:

- Provision of QoS for wireless multimedia applications where the mobile agent may be in the form of a user's proxy moving along with the mobile user in the corresponding wired network and may provide dynamic service adaptation and tailoring to the user device depending on the device and network constraints.
- Provision of personalized services to the portable device that uses the same proxy based approach to provide information based on the user's profile.
- Wireless distributed E-commerce applications; for example, banking services for portable devices.

REFERENCES

[1] L. Zhou and Z. J. Haas - Securing ad hoc networks. IEEE Network, Vol. 13, Nov.-Dec. 1999, pp. 24 –30, 1999.
[2] H. Luo, P. Zerfos, J. Kong, S. Lu, and L. Zhang – Selfsecuring Ad Hoc Wireless Networks. Proc. 7th Int. Symposium on Comp. and Communications (ISCC'02), 2002.
[3] R. Puttini, L. Me, R. de Sousa, "Certification and Authentication Services for Securing Manet Routing Protocols", accepted for publication in 5th IEEE Int. Conf. on Mobile and Wireless Communications Networks (MWCN2003), Oct. 2003.
[4] Y. Zhang and W. Lee – Intrusion detection in wireless ad hoc networks. Proc. 6th ACM Int. Conf. on Mobile Computing and Networking (MOBICOM 2000), pp. 275-283, 2000.

[5] Puttini, R; Percher, JM; Me, L, Camp, O; de Sousa, R. "A Modular Architecture for a Distributed IDS for Mobile Ad Hoc Networks". Lecture Notes on Computer Science vol. 2669, Springer-Verlag, pp. 91-113, 2003.

[6] K. Ilgun, R. A. Kemmerer, and P. A. Porras – State Transition Analysis: A Rule-Based Intrusion Detection Approach. IEEE Trans. on Software Engineering, pp. 181-199, March 1995.

[7] J. Cabrera, L. Lewis, R. Prasanth, X. Qin, W. Lee, and R. Mehra – Proactive detection of distributed denial of service attacks using MIB traffic variables – a feasibility study. Proc. 7th IFIP/IEEE Int. Symposium on Integrated Network Management, Seattle, WA, USA, may 2001.

[8] S. Staniford-Chen, and L. Heberlein – Holding Intruders Accountable on the Internet. Proc. 1995 IEEE Symposium on Security and Privacy, 1995.

[9] F. Wang, F. Wu – On the vulnerabilities and Protection of OSPF Protocol. Proc. 1998 Int. Conf. on Computer Communications and Networks, 1998.

[10] W. Jansen. Intrusion Detection with Mobile Agents. Computer Communications 25(15), Special Issue on Intrusion Detection, Elsevier, pp. 1392-1401, September 2002.

[11] H. Debar, M. Dacier and A. Wespi - A revised taxonomy for intrusion-detection systems, IBM Research Report, 1999.

[12] W. Lee; S. J. Stolfo; and K. W. Mok - A data mining framework for building intrusion detection models. Proc. 1999 IEEE Symposium on Security and Privacy, 1999.

[13] D. Curry, H. Debar, and Merrill Lynch – Intrusion Detection Message Exchange Format Data Model and Extensible Markup Language (XML). IETF Internet draft. June 2002.

[14] H. Yang, X. Meng and S. Lu, "Self-Organized Network Layer Security in Mobile Ad Hoc Networks", Proc. ACM Workshop on Wireless Security – 2002 (WiSe'2002), in conjunction with ACM MOBICOM2002, September, 2002.

[15] T. Clausen, P. Jacquet, A. Laouiti, P. Minet, P. Muhlethaler, A. Qayyum, L. Viennot - Optimized Link State Routing Protocol - IETF Internet Draft, MANET working group, version 11, Jul. 2003.

[16] K. McCloghrie; and A. Bierman - Entity MIB (Version 2). IETF Request for Comment 2737, December 1999.

[17] J. Kiniry and D. Zimmerman - Special Feature: A Hands- On Look at Java Mobile Agents. IEEE Internet Computing, Vol. 1, No. 4, July/August 1997.

[18] G. Helmer, J. Wong, V. Honavar, L. Miller, Y. Wang – Lightweight Agents For Intrusion Detection. To be published in The Journal of Systems and Software.

[19] S. Gwalani, E. Royer, G. Vigna, R. Kemmerer – AODVSTAT: Intrusion Detection in AODV (work in progress)

[20] P. Mell, D. Marks, M. McLarnon – A Denial-of-Service Resistant Intrusion Detection Architecture. Computer Networks, Special Issue on Intrusion Detection, Elsevier Science BV, November 2000.

[21] Ricardo Puttini, University of Brasilia – Brasilia – Brazil, Ludovic Mé Supélec - Rennes – France, Jean-Marc Percher ESEO - Angers – France, Rafael de Sousa University of Brailia - Brasilia – Brazil

[22] Chandra Krintz, Security in agent-based computing environments using existing tools. Technical report, University of California, San Diego, 1998.

[23] Neeran Karnik. Security in Mobile Agent Systems. PhDthesis, Department of Computer Science and Engineering. University of Minnesota,1998.

[24] Joshua D. Guttman and Vipin Swarup. Authentication for mobile agents. In LNCS, pages114–136. Springer, 1998

[25] Tomas Sander and Christian F. Tschudin. Protecting Mobile Agents Against Malicious Hosts.In Giovanni Vigna, editor, Mobile Agent Security, pages 44–60. Springer-Verlag: Heidelberg,Germany, 1998.

[26] Puttini R. and jean-Mare Percher-"A Fully Distributed IDS for MANET",IEEE Int.Conference ,2004.

[27] S.Hofmeyr,S.Forrest-Architecture of an Artificial Immune System.Evolutionary Computation 7(1), Morgan-Kaufmann,San franciscp, CA,pp.1289-1296(2000).

[28] S.Fenet, S,Hassas-A Distributed Intrusion Detection and response System Based on Mobile autonomous Agent Using Social Insects CommunicationParadiagms.Proc.1st Int.Workshop on Security of Mobile Multiagents Systems,2001.

[29] D. Barman Roy1 and R. Chaki" MADSN: Mobile Agent Based Detection of Selfish Node in MANET" International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 4, August 2011.

[30] Panthi N.K. et al. / (IJCSIT) International Journal of Computer Science and Information Technologies, "Securing Mobile Agent Using Dummy and Monitoring Mobile Agents" Vol. 1 (4) , 2010, 208-211.

[31] Kumar R. and Dr. Dave M." Mobile Agent as an Approach to Improve QoS in Vehicular Ad Hoc Network" IJCA Special Issue on "Mobile Ad-hoc Networks"MANETs, 2010.

[32] Saidat Adebukola Onashoga, A Strategic Review of Existing Mobile Agent-Based Intrusion Detection Systems, Issues in Informing Science and Information Technology Volume 6, 2009.

[33] Zeng-Quan Wang And Hui-Qiang Wang "Research On Distributed Intrusion Detection System", IEEE,Proceedings of the Fifth International Conference on Machine Learning and Cybernetics, Dalian, 13-16 August 2006.