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

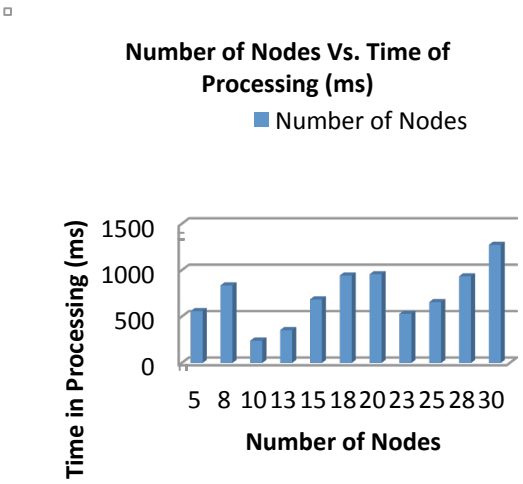
In our experimental results shows the proposed algorithm is expected to perform better in all situations as: The algorithm proposed is used to study the behaviour of mobile agents. This study is based on important Internet applications where they are believed to have better performance. Following measures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

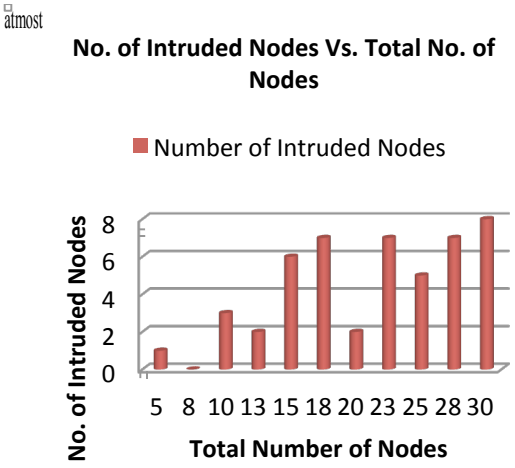
From the simulation performed following data table1 has been generated which shows the various topologies applied to test the simulation for accuracy and security

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*

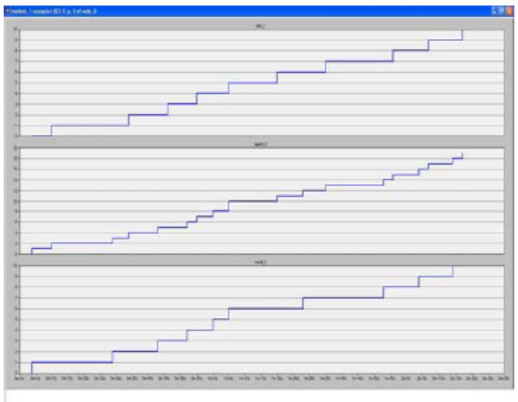


Figure 2: Simulation result for 12 nodes where 1 node is suspicious (total simulation time 300 seconds).

B. Simulation Result for Faulty Nodes

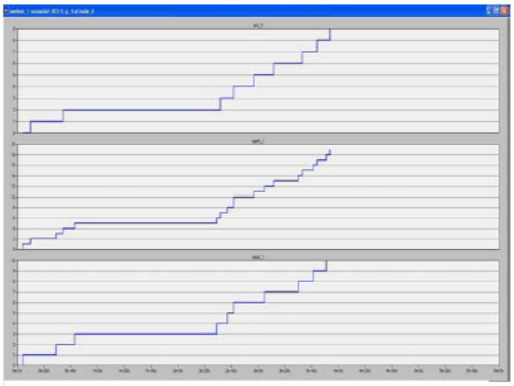


Figure 4: Simulation result for 12 nodes where 1 node is faulty (total simulation time 6.5 minutes).

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.