Volume 4, No. 8, May-June 2013

ISSN No. 0976-5697

International Journal of Advanced Research in Computer Science

RESEARCH PAPER

Available Online at www.ijarcs.info

Secure Agent Base Data Transmission in MANET

J. K. Mandal
Department of Computer Science and Engineering,
University of Kalyani, Kalyani,
Nadia-741235, West Bengal, India,
jkm.cse@gmail.com

Khondekar Lutful Hassan
Department of Computer Science and Engineering,
University of Kalyani, Kalyani,
Nadia-741235, West Bengal, India,
klhassan@yahoo.com

*Abstract***:** In this paper an agent base secure data transmission technique in MANET has been proposed. In this approach Triangular encryption (TE) technique is applied for encryption and decryption purposes. Agents are encrypted by the source node before forwarding. Upon reaching the destination node the agents are automatically decrypted. If any node captures the agent the packet will be dropped without decrypting the agent. The technique is applied for both AODV and DSR routing protocols in MANET. For simulation purpose NS2 (2.33) is taken and two types of parameters are considered. These are number of nodes and types of routing protocol. Various analysis have been done through which it is established that this technique can be used to transmit packets in MANET with a high degree of security without affecting the performance of the routing protocols. The parameters which are considered for the performance comparison of both protocols are Number of packets generated, average packet size, processing times, retransmitted data and average delay.

Keywords: Triangular Encryption Technique (TE), Secured Agent, MANET, NS2, Secure Transmission.

I. INTRODUCTION

MANET [1, 2, 3] consist of set of dynamic nodes which are capable to routing also.There are three types of routing protocols, they are proactive, reactive, and hybrid routing protocols. Proactive routing protocols are those types of protocols which initiate continuously to evaluate the routes so that when a packet needs a root it can be used immediately. In this case, nodes keep tables with information about the network and react in topology changes, propagating updates in order to maintain the network consistency, DSDV [1,2,3,4,5] is the example of proactive routing protocols. On the other hand reactive routing protocols are those protocols which creates the routing table when it require thus this type of routing protocols are called on demand. AODV [1,2,3,4,5]and DSR [1,2,3,4,5] are the example of this type of routing protocol. Hybrid protocols are combining the advantages of proactive and reactive routing protocols. The routing is initially established with some proactively prospected routes and then serves the demand from additionally activated nodes through reactive flooding. ZRP is the example of hybrid routing protocols.

Agent is the software entity which can move from one node to another node for performing a define task

Security is a very challenging issue in MANET because of node mobility. As the MANET, [1, 2, 3] are very dynamic in nature. So maintenance of wireless network is very hard but wired network is static so security manager can handle its task very easily because all nodes are fixed. There are many cryptographic algorithms which are implemented for secure data transmission in network. In this paper it is going to describe the implementation the secure agent base data transmission in MANET [1, 2, 3]. For this purpose it is considered Triangular Encryption Technique (TE)[9,10] for encryption and decryption . Triangular Encryption Technique (TE)[9,10] is a key less encryption. A mobile agent has been initiated for secure data transmission .encrypted data is associated with the agent by the source node and the same will be decrypted automatically when it reaches the destination. If don't reach the destination then it will be dropped but not decrypted. If unauthorized node captures the agent then the data will not be decrypted but the agent will be dropped so the data will be secured and there will not be leakage of any data. Network Simulator 2(NS2) [6, 7] is taken as the simulation tool. With this technique it is tried to enhance the security in the network

Section II of the paper deals with the proposed technique. Simulation environment has been presented in section III. Section IV deals with simulations. Results and comparison of performance are described in section V. And conclusion is drawn in section VI.

II. PROPOSED TECHNIQUE AND METHODOLOGY

For agent base secure data transmission data transmission it is required to create mobile agent which is secure. For this purpose the agents need to be encrypted in source node and decrypted to the destination node.

In proposed scheme any routing protocol may be consider, because routing protocols are responsible for creating the root here. The focus is to create an agent which is secure. For this purpose a Sec_Agent protocol has been written and then bitwise Triangular Encryption (TE)[9,10] Technique is added with Sec_Agent protocol.

The process of triangular encryption is described is as follows. Consider a block S= s^0_0 s^0_1 s^0_2 s^0_3 s^0_4 s^0_5 ..... s^0_{n-2} s^0_{n-1} of size n bits , where s^0_1 = 0 or 1 for 0<=i<=(n-1).Starting from MSB (s^0_0) and the next to MSB (s^0_1), bits are pair-wise XNORed, so that the first intermediate sub-stream S^1 = S= s^1_0 s^1_1 s^1_2 s^1_3 s^1_4 s^1_5 ..... s^1_{n-2} s^1_{n-1} is generated

consisting of (n-1) bits, where $s^1_j = s^0_j$ (XNOR) s^0_{j+1} for 0<=j<=n-2.The first intermediate sub stream S^1 is also pair-wise XNORed to generate $S^2=s^2_0\ s^2_1\ s^2_2\ s^2_3\ s^2_4\ s^2_5 \ldots\ s^2_{n-2}\ s^2_{n-1}$, which is the second intermediate sub-stream of length (n-2). This process continues (n-1) times to ultimately generate $S^{n-1}=S^{n-1}_0$, which is a single bit only. Thus the size of the first intermediate sub-stream is one bit less than the source sub-stream; the size of each of the intermediate sub-stream starting from the second one is one bit less than that of the sub-stream wherefrom it was generated and finally the size of the final sub-stream. Figure 1 shows the generation of the intermediate sub-stream $S^{j+1} = s^{j+1}_0\ s^{j+1}_1\ s^{j+1}_2\ s^{j+1}_3\ s^{j+1}_4\ s^{j+1}_5 \ldots\ s^{j+1}_{n-(j+2)}$ from the previous intermediate sub-stream $S^j= s^j_0\ s^j_1\ s^j_2\ s^j_3\ s^j_4\ s^j_5 \ldots\ s^j_{n-(j-1)}$. The formation of the triangular shape for the source sub-stream $S= s^0_0\ s^0_1\ s^0_2\ s^0_3\ s^0_4\ s^0_5 \ldots\ s^0_{n-2}\ s^0_{n-1}$ is shown in figure 1

$$S= s^0_0\ s^0_1\ s^0_2\ s^0_3\ s^0_4\ s^0_5 \ldots\ldots\ldots\ldots\ s^0_{n-2}\ s^0_{n-1}$$
$$S^1 = s^1_0\ s^1_1\ s^1_2\ s^1_3\ s^1_4 \ldots\ldots\ldots\ldots\ s^1_{n-2}$$
$$S^2= s^2_0\ s^2_1\ s^2_2\ s^2_3 \ldots\ s^2_{n-3}$$
$$\ldots\ldots\ldots\ldots\ldots$$
$$S^{n-2} = s^{n-2}_0\ s^{n-2}_1$$
$$S^{n-1} = s^{n-1}_0$$

Figure.1. Formation of triangle in traingular encryption (TE)

Using the triangular encryption (TE) [9, 10] technique the agent are encrypted and then the encrypted agent are send from the source node. As triangular encryption (TE) technique is a key less encryption technique so it is not required any key to send to the destination node. The only understanding between nodes are to be made is the six of the block .When the encrypted node reached to the destination node then the encrypted agent are decrypted applying same method as given in figure 1. Thus the original massage is regenerated by the destination node. If the agent (data) reaches the destination then it will be decrypted. If any node capture the Agent then it will not decrypted. The agent can be decrypted if and only if the agent reaches to the destination. Figure 2 shows the pictorial representation of the proposed technique.

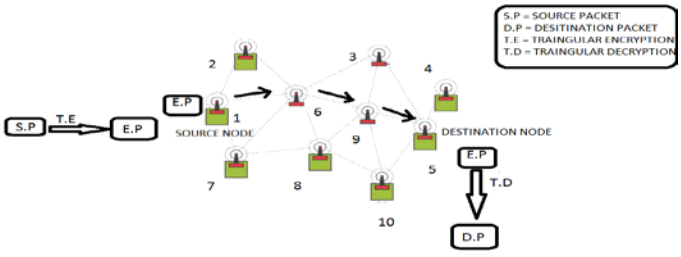

Figure 2. Pictorial representation of proposed technique

III. SIMULATION ENVIRONMENT

For simulation purpose Network Simulator (NS2)[6,7] is taken . NS2 is an event driven simulation. NS2 is combination of two languages namely OTCL and C++. OTCL work on frontend for setting up simulation by assembling and configuring the objects as well as scheduling discrete events work in back end to maintain internal mechanism and C++ is used back end for internal mechanism and configuration. After simulation trace file and nam file is generated. Nam file is used for animation and trace file consist about all information of all events. Trace file used for mathematical analysis.

IV. SIMULATION

For the purpose of simulation various parameters are taken for simulation and some metrics are considered for result analysis and comparison after simulation.

A. Parameter of simulations:

For the purpose of simulation five parameters are taken as common in each case and two parameters are taken as variable parameters for comparison of the performance of the network with applying this technique. Table 1 show the fixed parameters which are taken as common in each cases

Table 1 fixed parameter of the simulation.

Routing protocols	**AODV**
% of node mobility	40 %
Maximum packets in IFQ	50
Speed of the nodes	100 m/s
Time of simulation	10 sec

Variable parameters are

a. No of Nodes : 20, 30, 40, 50 and 60

b. Routing Protocols : AODV and DSR

Snapshots of the simulations are shown in the figure 3 and 4 respectively.

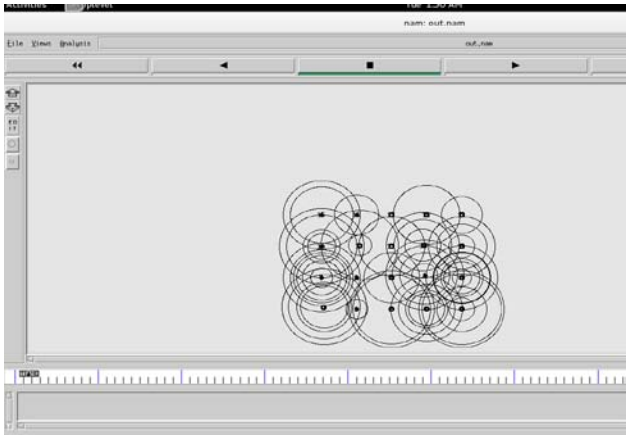

Figure 3. Nam view of the simulation

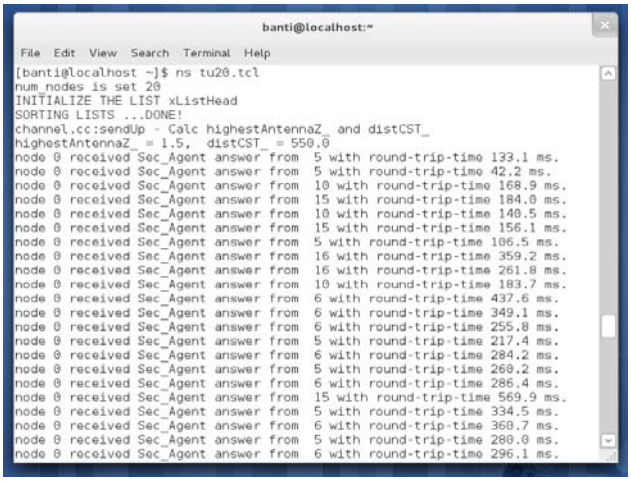

Figure 4. Output snap shot in terminal window

B. Performance metrics:

The performance metrics used to evaluate the efficiency of the network using proposed scheme for the performance analysis six parameters are considered as performance metric, which are given bellow.

a) Packet Generated
b) Average Packet Size
c) Processing Time
d) Retransmitted Data (Byte)
e) Average End To End Delay

Packet generated metrics are considered here total number of Sec_Agent packets are generated in the total simulation time(10 sec) throughout the network and also packet drop considered here total number of all type of packets including broadcast packets are dropped in the simulation. Retransmitted data are amount of total data in Bytes which are retransmitted in the simulations

V. PERFORMANCE ANALYSIS AND COMPARISONS

A. Packet Generated:

Comparison of number of total number of Sec_Agent packets are generated in both AODV and DSR routing protocols are shown in the figure 5

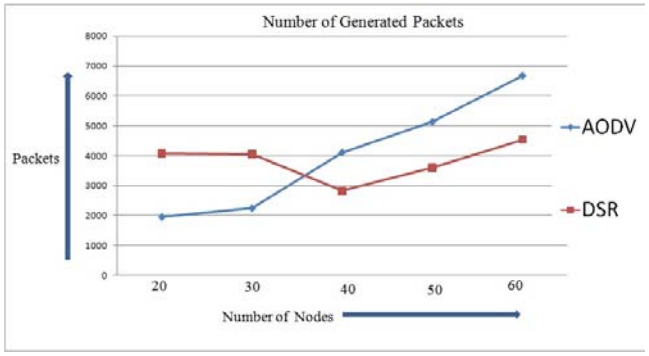

Figure 5. Number of Generated Sec_Agent packets

From the figure 5 it is seen that when the number of nodes are 20 and 30 DSR generated more Sec_Agent packets, but when the nodes number are above 30 then AODV generated more Sec_Agent packets.

B. Average Packet Size:

Comparisons of average packet size in the both routing protocols are showing in the figure 6.

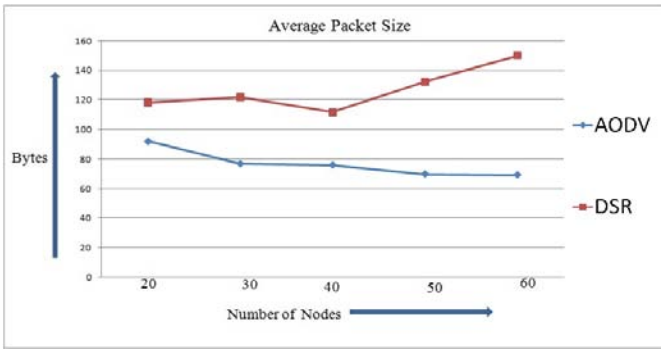

Figure 6. Average Packet size in the both protocols

Figure 6 shows that average packet size of DSR is higher than AODV in any node densities.

C. Processing Time:

Comparisons of processing time are showing in the figure 7

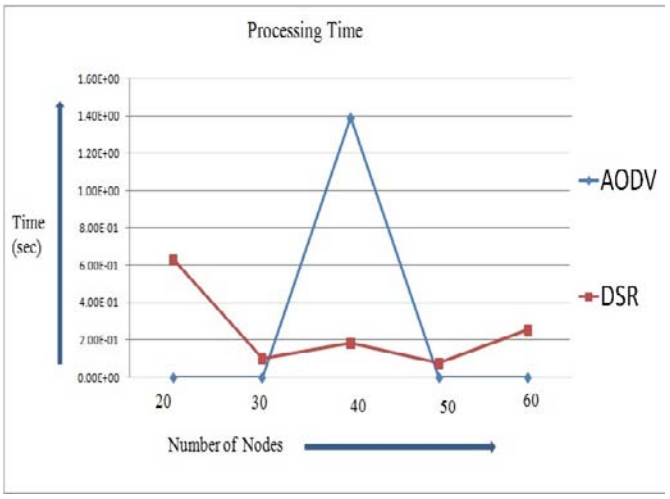

Figure 7. Processing time in AODV and DSR with various node densities.

Figure 7 represent that processing time of AODV is very less than DSR. But when the node number is 40 at that time processing time of AODV is changed rapidly, it can be cause for any other parameters.

D. Retransmitted Data(Byte):

Both AODV and DSR have retransmitted same amount of data. Comparison of retransmitted data (Byte) is showing in the figure 8.

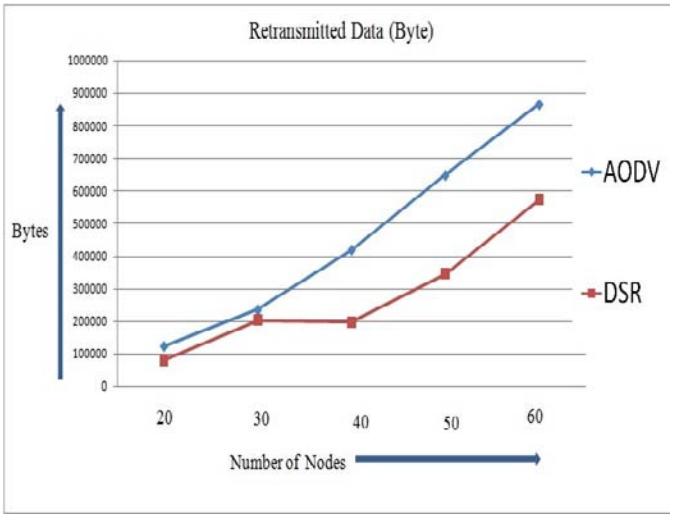

Figure 8. Comparison of retransmitted data in both routing protocols.

Figure 8 represented that AODV retransmitted more data than DSR. So packet drop in DSR is less than AODV.

E. Average End To End Delay:

Average end to end delays of data (Sec_Agent packets) transmission in the both routing protocols are shown in the figure 9.

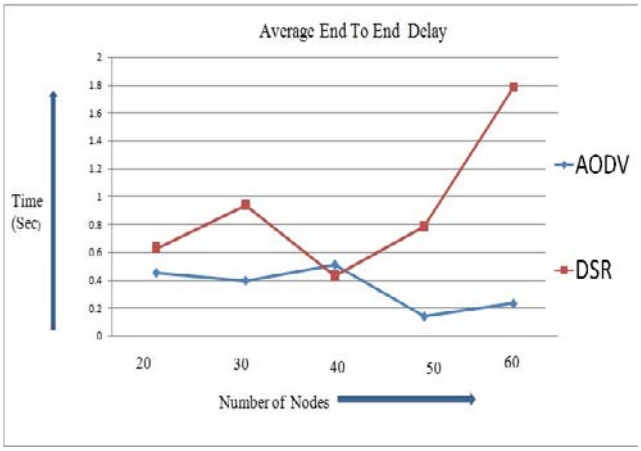

Figure 9. Average End to End delay in the both protocols

From the figure 9 it is seen that end to end delay of DSR is very high compared to AODV. When number of nodes is 40 at that time end to end delay of both protocols are more or less same.

VI. CONCLUSION

In this paper a secured agent based data transmission technique has been applied in both AODV and DSR routing protocols and the performance analysis and comparison are performed in detail. Although Triangular Encryption method is an establish method but this Triangular Encryption (TE) is applied to encrypt the agent in MANET [1, 2, 3, 4, 5], for time efficiency and less computational complexity of the technique.

Proposed technique has been applied in multiple routing protocols (AODV and DSR) .The specialty of this method is that if the agent (data) reach the destination then it will be decrypted. If any node other than the destination node capture the Agent then it will not decrypted. Only the agent can be decrypted itself if and only if the agent reaches to the destination. That is why the data are more secured than other traditional techniques [11, 12, 13, 14, 15]. Thus the security of the MANET is enhanced using this technique without affecting any routing protocols.

VII. ACKNOWLEDGMENT

The authors expressed deep sense of gratuity towards the Depment of Computer Science & Engineering, University of Kalyani where the computational resources are used for the work under the PURSE scheme of DST, Government of of India.

VIII.REFERENCES

[1] C.Siva Ram Murthy and B.S manoj" Ad Hoc Wireless networks architecture and protocols" Pearson education india 2005.

[2] Prasant Mohapatra, Srikanth Krishnamurthy "Ad hoc networks: technologies and protocols" Springer; 2005 edition (September 23, 2004)

[3] Chai-Keong Toh "Ad hoc mobile wireless networks: protocols and systems " Prentice Hall, Web ISBN-13: 978-0-13-244270-1 , December 03, 2001.

[4] Amitava Mishra "Security and Quality of Service in Adhoc Wireless Network", Cambridge University Press , ISBN-13: 978-0521878241 , March 17, 2008.

[5] Sarkar, S.K., Basavaraju, T.G., Puttamadappa, C.: Ad hoc Mobile Wireless Networks: Principles, Protocols and Applications. Auerbach Publications (2008)

[6] Teerawat Issariyakul, Ekram Hossain "Introduction to Network Simulator NS2" Springer (2009)

[7] Marc Greis' Tutorial http://www.isi.edu/ nsnam/ns tutorial/, accessed on 31st march 2013.

[8] Mubashir Husain Rehmani, Sidney Doria, and Mustapha Reda Senouci "A Tutorial on he Implementation of Ad-hoc On Demand Distance Vector (AODV) Protocol in Network Simulator (NS-2)"

[9] Mandal J. K.,Dutta, S.,Mal, S., "A Multiplexing Triangular Encryption Technique – A Move Towards Enhancing Security in E-Commerce, Proc. of Conference of Computer Association of Nepal, December, pp 120-132, 2001.

[10] Mandal, J. K., Chatterjee R, "Authentication of PCSs with Triangular Encryption Technique", Proceedings of 6th Philippine Computing Science Congress(PCSC), Ateneo de Manila University, Manila, Philippine, March 28-29,2006.

[11] Li Zhao and José G. Delgado-Frias" Multipath Routing Based Secure Data Transmission in Ad Hoc Networks" Wireless and Mobile Computing, Networking and Communications, (WiMob). IEEE International Conference . pp 17-23, 2006.

[12] Rawat, A.; Vyavahare, P.D.; Ramani, A.K." Improved System Components for Secure Data Communication in MANETs using Secured DSR" Wireless Communication and Sensor Networks, WCSN,Third International Conference. Pp. 61-64, 2007.

[13] Jaisankar, N.; Saravanan, R.; Swamy, K.D." An agent based security framework for protecting routing layer operations in MANET", Networks and Communications, 2009. NETCOM . First International Conference. Pp. 381-385, 2009.

[14] R.Sivakami, Dr.G.M.Kadhar Nawaz," Secured Communication for MANETS in Military", International Conference on Computer, Communication and Electrical Technology – ICCCET, pp 146-151, 2011.

[15] B.Thanikaivel, B. Pranisa" Fast and Secure Data Transmission in MANET", International Conference on Computer Communication and Informatics (ICCCI), pp. 1-5,2012.