TRUST BASED INTRUSION DETECTION SYSTEM USING FUZZY TECHNIQUE AND ANT BASED AUTHENTICATION IN MANET

J. Godwin Ponsam and R. Srinivasan
SRM Institute of Science and Technology University, Chennai, India
Email: jgodwinsam@gmail.com

ABSTRACT

The focus of this work is to propose a integrated trust based detection and authentication based on ANT based authenticated Routing in MANET. Our trust management system combines the grey theory and fuzzy sets for calculating the trust value. This trust management framework designed to be robust against many attacks. Based on fuzzy based grey theory trust value is calculated. After trust value is calculated Ant based Authenticated routing is used to transmit a packet from source node to the destination node. Ant colony based routing algorithm (ARA) is used for routing the data packets. This routing algorithm is consists of three phases, route discovery, route maintenance and route failure handling. During route discovery phase new routes will be created. FANT will establish the pheromone track to the source node where else BANT will establish the pheromone track to the destination node. When source node sends the data it includes FA with a trust value included to it. The movement of FA will be decided based on the decision rule. FA moves by using the rule and will verify the trust value of the visited node is greater than trust threshold value. When FA reaches the destination BA will be generated and the information collected by FA will be given to BA. The BA takes the same path which FA used to reach the destination. Based on simulation results we show the proposed. Trust based Intrusion detection system using fuzzy technique and ANT based Authentication in MANET enhances the secure data communication.

Keywords: MANET, authentication, IDS, attacks.

1. INTRODUCTION

MANETs (Mobile Adhoc Networks) is one of the communication standard for wireless communication. Wired networks needs infrastructure to perform any communications where else MANET does not require any infrastructure to do any communication. It's a infrastructure less based network. MANET is defined a collection of autonomous nodes which forms a infrastructure less communication. In MANET each node will act a router node also as an end node. Each node will have capability to route the packet towards destination. All the nodes can communicate to other nodes in its range. Also outside node can be communicated using multihop communication. MANETs can be used for various applications like Military, Emergency and rescue operations.

1.1 Attacks in MANET

Due to dynamic nature of MANET its susceptible to both passive and active attacks. In passive attacks it leads to eavesdrops the data and in active attack replication and modification of data may happen. In MANET attacks may happen in any layer of the protocol suite. Some attacks are black hole attack, worm hole attack, byzantine attack, denial of service attack etc.

1.2 Intrusion detection system

The responsibility of an Intrusion detection system (IDS) is to monitor the activities happening in a network. The main functionality of the IDS is to detect the abnormal activities happens in a network by analyzing the data.

IDS are basically categorized into standalone IDS, Distributed and Cooperative IDS and Hierarchical IDS.

In the standalone IDS the IDS will be running on each node to detect intrusions. In the distributed and cooperative IDS the IDS will be distributed across the network. An IDS agent which runs to detect the intrusion happens in that network. Hierarchical IDS the network will be divided into clusters. Each node there will be an agent which monitors and detects the intrusions locally and informs to the cluster head. Cluster head will monitor the nodes in its control and also informs as the global response.

1.3 Issues of IDS

There are lot of IDS available but still lacking due to mobility in nodes and also nodes are more vulnerable can be easily compromised [4]. Its difficult to decide intrusions as the nodes are dynamically changing the topology.

2. RELATED WORK

Trust management can be done either using centralized authority or using nodes or both in combined. Kamel Adi proposed a trust establishment scheme based on self certification [11]. Zhou proposed threshold cryptography to distribute the trust [12]. Davis proposed a trust model based on hierarchical trust model to manage the trust [13]. N. Li and S. K. proposed a trust management framework [14]. Marshall and Zhou proposed a trust management scheme based on fuzzy set [15]. But this scheme is used for static with limited parameters. Three are lot of research done by Mishra about the different types of IDS architecture. But still analysis about the detection is not done. Zhang proposed a model for measuring the efficiency of IDS. zhang evaluated the application based intrusion detection architecture but for assessing the model detection, accuracy and false alarm parameters are used. James Cannady proposed an approach to detect the attacks in MANETs [16]. His technique enables to detect attacks in a distributer manner. This helps to detect the complex attacks agains MANETs. Aikaterini Mitrokotsa [17] *et al* proposed an IDS where local agents sends detection information. Their technique will classify the normal and abnormal behavior based on MAC layer.

2.1 Proposed solution

In this paper we propose a Trust based Intrusion detection system using fuzzy technique and ANT based Authentication in MANET. The trust management system combines the grey theory and fuzzy sets for calculating the trust value. When a source node wants to communicate with the destination node based on the trust value the packet is routed towards destination.

Our trust management system combines the grey theory and fuzzy sets for calculating the trust value. This trust management framework designed to be robust against many attacks.

2.2 Grey theory

Based on grey theory we can calculate the trust value. From Grey theory, let there be a grey relational set x={x1, x2, x3….xn}. x= {packet loss rate, signal strength, packet delivery rate, delay, throughput}.

After some time period from the view of a node x which observes the neighbor node a and calculates its trust value. This framework will get the nodes sample sequence xi. After some time period t, the best trust value sequence A=(a1,…ai…an) while ai= best chosen value. Also the worst value sequence B=(b1,…bi…bn).bi is the worst chosen value. Based on Grey theory we can obtain the Grey relation coefficient of the best trust value and worst trust value.

$$\{\theta,\varphi\}=\frac{\mathrm{minj}|\partial ji-\{a,b\}i|+\rho\,\mathrm{maxj}|\partial ji-\{g,b\}i|}{\partial|ji-\{a,b\}i+\rho\,\mathrm{maxj}|\partial ji-\{a,b\}i|} \qquad (1)$$

At time period t, node b’s best and worst value will be

$$\{\ \theta,\varphi\ \}j=\Sigma_i=vi\{\theta,\Phi\}j,I \qquad (2)$$

Trust value Computation

The overall trust value is computed based on fuzzy set. We followed the approach to identify the trust of a node based on its historical behavior and we get the trust value based on classes of grey clusters.

The following are the classes of grey clusters.

A1 Not trusted
A2 Min trust
A3 Trusted

When node x gets trust value of node y from different nodes. The Whitenization weight of trust value TxK. TxK is the trust value of x evaluated by node k.

$$f1(x)=\begin{cases} 1, x <= .30 \\ -4x/3+4/3, x > .25, \end{cases} \qquad x1=.25$$

$$f2(x)=\begin{cases} 2x, x <= .5 \\ -2x+2, x > .5, \end{cases} \qquad x2=.5$$

$$f3(x)=\begin{cases} 4x/3, x <= .75 \\ 1, x > .75, \end{cases} \qquad x3=.75$$

When node x gets trust value of node y from different nodes. The Whitenization weight of trust value TxK. TxK is the trust value of x evaluated by node k.

$$\mathrm{Tjk}=\frac{1}{1+(\varphi j)^2}\ /\ (\theta)^2 \qquad (4)$$

If maxs{fs(TBK)} is between certain value grey cluster class is A2,

If maxs{fs(TBK)} is under the value then A1 then not quite trusted

If maxs{fs(TBK)} is above the value then the class is A3 quite trusted.

The total trust value for node K is

$$\text{Total } T=\frac{1}{2}(\max\{fj(\mathrm{Tdirect})\})+\frac{1}{2}\ \frac{2NR}{2NR+N1}\ \Sigma\ \frac{wk}{\Sigma wk}(\max\ \{fj(Tk)\})Tk+ \frac{1}{2}\ \frac{N1}{2NR+N1}\ \Sigma\ \frac{wk}{\Sigma wk}(\max\ \{fj(Tk)\})Tk \qquad (5)$$

ANT authenticated routing

ARA is a protocol which does routing after route discovery. Also takes cares of route maintenance and route handling. New routes will be created during route discovery process using forward Ant (FANT) and backward ANT (BANT). An agent runs as a FANT will generate pheromone track. This helps to reach back the source node. BANT generates the pheromone track back to the destination node. FANT computes the pheromone value based on number of hops it took to reach the destination node. Destination node will create the BANT and ruturns it to the source node. When the source node receives the BANT it sends the data to the destination node.

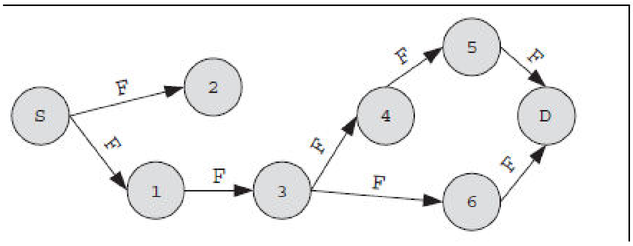

Figure-1. Route discovery.

Handling route failure

Because of node mobility route failure may happen. If node receives a route failure message then it will deactivate that link by setting pheromone value 0. Then the node search any alternate route is available in routing table. If there is alternate route available then it will send the packet using alternate route. If no route available then the source node initiates the discovery process.

2.3 Trust based detection and ANT based authentication routing in MANET

When source node sends the data it includes FA with a trust value included to it. The movement of FA will be decided based on the decision rule. FA moves by using the rule and will verify the trust value (T) of the visited node is greater than trust threshold value (T_{Th}). The Fig. shows the movement of Forward ANT and Backward ANT. Then FA will continue its path and keeps the Each FA will deposit some pheromone based on the equation. When FA reaches the destination BA will be generated and the information collected by FA will be given to BA. The BA takes the same path which FA used to reach the destination. It will update the pheromone table with the trust value of that node Ni. Once source reaches the BA it collects the routing information about all Ni along each path from its updated pheromone table. From the information received Source chooses the route with trusted nodes for data communication.

$$Ti < Tth \tag{6}$$

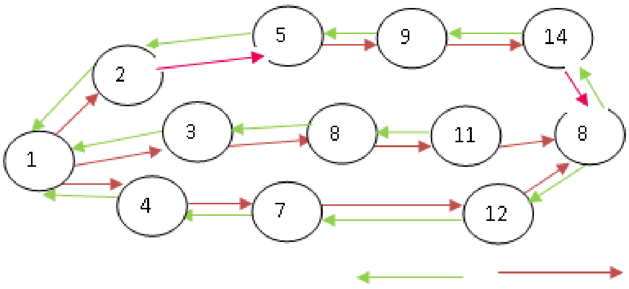

Figure-2. Movement of forward ant and backward ant.

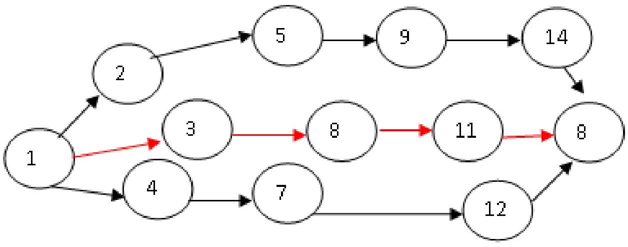

Figure-3. Ant based authenticated routing.

The above Fig. shows the authenticated route from source to destination. 1-3-8-11-13

3. SIMULATION RESULTS

We have used NS2 to simulate our algorithm. We have set the channel capacity to 1 Mbps. Mobile nodes will move in 1000 x 1000 meter for 100 seconds. The nodes speed was set at 10m/s. The traffic set for simulation is CBR

No. of Nodes	20
No. of attackers	1 to 5
Mac	802.11
Simulation Time	100sec
Traffic	CBR
Speed	10m/s
Attackers	5
Routing Protocol	TBDAR

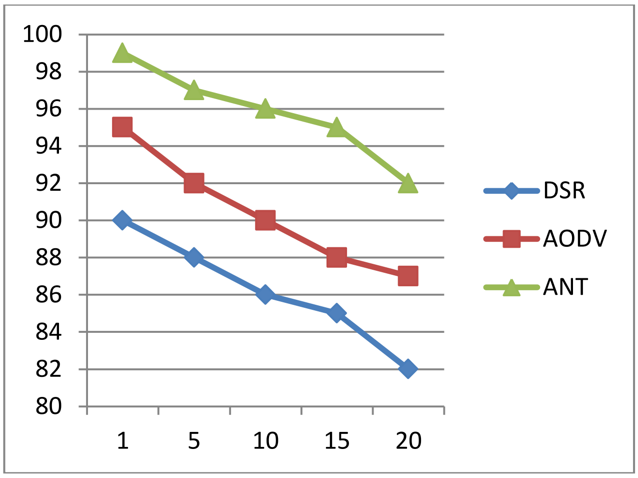

Figure-4. PDR vs mobility rate.

In the first experiment the delivery ratio of the ANT based routing is higher than the AODV routing protocol and DSR routing protocol.

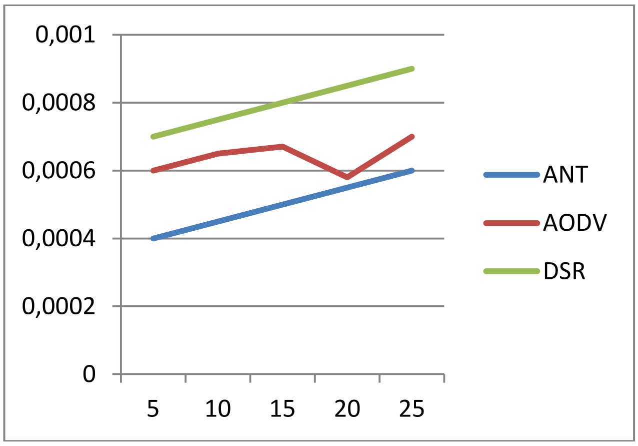

Figure-5. Delay vs mobility rate.

Trust based detection and ANT based authentication routing in MANET

No. of Nodes	100
Area size	1000x1000
Transmission Range	250m
Simulation Time	1000 seconds
Packet Size	512
Speed	10 m/s
Traffic Source	CBR

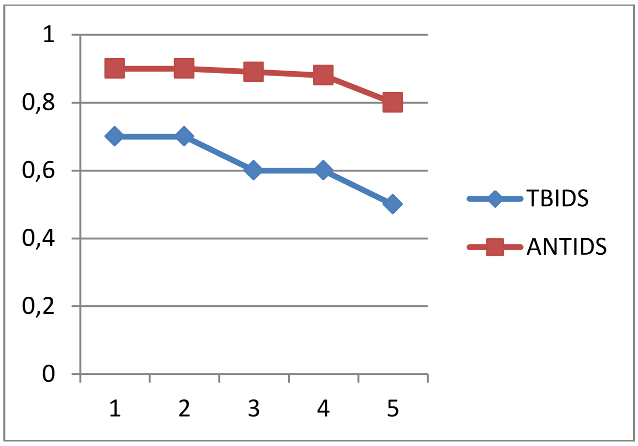

Figure-6. Attackers vs delivery ratio.

In the above experiment we have changed the no. of attackers as 1, 2, 3, 4 and 5.

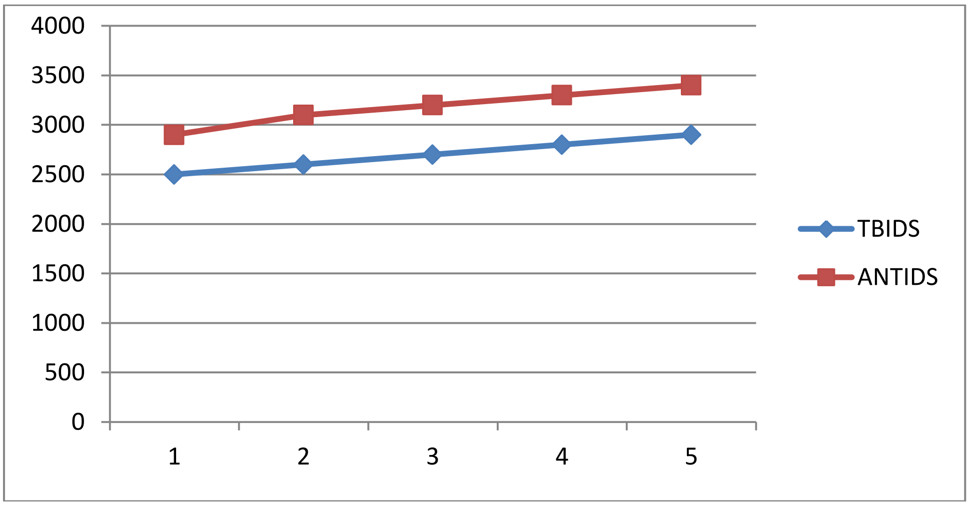

Figure-7. Attackers vs throughput.

In the above experiment the graph shows that delivery ratio of our proposed algorithm is higher when compared to trust based intrusion detection system.

4. CONCLUSIONS

In this paper we have proposed Trust based Intrusion detection system using fuzzy technique and ANT based Authentication in MANET. The trust value is calculated based on grey theory and fuzzy set. When a node wants to transmit a packet to a destination node the route with trusted nodes is selected using ant based technique. Using simulation results we have shown proposed technique has good delivery ratio and detection rate.

REFERENCES

[1] J.Godwin Ponsam, R.Srinivasan. 2015. Trust Management Scheme for MANET. International Journal of Applied Engineering Research. 10(9).

[2] J. Godwin Ponsam, R. Srinivasan. 2015. Multilayer Intrusion Detection in MANET. IJCA. Vol. 98.

[3] J. Godwin Ponsam, R. Srinivasan. 2014. A Survey on MANET Security Challenges, Attacks and its Countermeasures, in IJETTCS.

[4] J. Godwin Ponsam, R.Srinivasan. 2016. Secure Key Management Scheme for MANET. European Journal of Scientific Research. 138(4).

[5] Muhammad Saleem, Gianni A. Di Caro, Muddassar Farooq. 2010. Swarm intelligence based routing protocol for wireless sensor networks:Survey and future directions. pp. 1-28.

[6] E. Bonabeau, M. Dorigo and G. Theraulaz. 1999. Swarm intelligence:from natural to artificial

intelligence. Oxford University Press. ISBN 0-19-513158-4

[7] M. Dorigo and G. Di Caro. 1999. The ant colony optimization meta-heuristic. In D. Corne, M. Dorigo, and F. Glover, editors, New Ideas in Optimization, pp. 110-32. McGraw-Hill, London.

[8] Mesut G¨unes, Udo Sorges, Imed Bouazizi. 2002. ARA- The Ant-Colony Based Routing Algorithm for MANETs. International Workshop on Ad Hoc Networking (IWAHN 2002), Vancouver, British Columbia, Canada.

[9] ShabanaMehfuz and M. N. Doja. 2008. Swarm Intelligent Power-Aware Detection of Unauthorized and Compromised Nodes in MANETs. Journal of Artificial Evolution and Applications. pp. 1-16.

[10] Wassim El-Hajj, Fadi Aloul, Zouheir Trabelsi. 2008. On Detecting Port Scanning using Fuzzy Based Intrusion Detection System. International wireless Communications and Mobile Computing Conference (IWCMC).

[11] Khaled Hamouid and Kamel Adi. 2012. Self-Certified Based Trust Establishment Scheme in Ad-Hoc Networks. International Conference on NTMS.

[12] L. Zhou and Z.J. Haas. 1999. Securing ad hoc networks. IEEE Network Magazine. 13(6): 24-30.

[13] C. Davis. 2004. A localized trust management scheme for ad hoc networks. Proceedings of 3rd International Conference on Networking (ICN'04).

[14] N. Li and S. K. Das. 2012. A trust-based framework for data forwarding in opportunistic networks. Ad Hoc Networks, Elsevier.

[15] J. Guo, A. Marshall and B. Zhou. 2011. A Trust Management Framework for Detecting Malicious and Selfish Behaviour in Ad-Hoc Wireless Networks Using Fuzzy Sets and Grey Theory. Springer. pp. 277-289.

[16] James Cannady. 2010. Dynamic Neural Networks in The Detection of Distributed Attacks in Mobile Adhoc Networks. International Journal of Network Security & Its Application (IJNSA). 2(1).

[17] Aikaterini Mitrokotsa1, Nikos Komninos2 and Christos Douligeris. 2010. Protection of an Intrusion Detection Engine with Watermarking in Ad Hoc Networks. International Journal of Network Security. 10(2): 93-106.