ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645
Indian Journal of Science and Technology, *Vol 8(S9), 223–227, May 2015* DOI: 10.17485/ijst/2015/v8iS9/58398

Agent Based Trust Estimation for Mobile Ad Hoc Network

M. B. Mukesh Krishnan[1*], T. Balachander[2] and P. Rajasekar[1]

[1]Department of Information Technology, SRM University, Kattankulathur, Chennai - 603 203, Tamil Nadu, India, mukeshkrishnan.mb@ktr.srmuniv.ac.in, rajasekar.p@ktr.srmuniv.ac.in
[2]Department of Computer Science and Engineering, SRM University, Chennai - 603 203, Tamil Nadu, India; balachander.t@ktr.srmuniv.ac.in

Abstract

This paper develops novel mechanisms for providing Agent Based Trust Estimation for Mobile Ad Hoc Network. The primary aim of the scheme is to provide trust among the nodes. The highlight of the developed trust scheme is to estimate the trust level of node without the knowledge of the node. The proposed mode has two agents deployed to estimate the trust of a node. The first agent keeps track of the network link failure and packet dropping. The second agent keeps track of attacks and malicious behavior in the network. The two agent based trust scheme provides the nodes to interconnect with the trusted nodes together which increases the level of quality of service for MANET environment. The proposed model is tested by comparing the other trust models and the results shows good improvement than the other trust models for MANET.

Keywords: Agent, Attacks, Link Failure, Malicious Node, MANET, Trust

1. Introduction

Mobile ad-hoc networks are self organized, self created and self managed networks without any basic infrastructure. They can be rapidly deployed and reconfigured. Set of applications for MANET is diverse ranging from small static networks that are constrained by power sources to large scale dynamic networks. Success in operations of a mobile ad hoc network depends on cooperation of the nodes in providing services to each other. Since mobile ad hoc network makes it possible for the devices to join or leave the domain without permission, makes the nodes in the domain as untrusted. Trust estimation is the main concern to provide the reliable communication. This paper concentrates to estimate the trust level of node using two agents. The first agent keeps track of the network link failure and packet dropping, which provides the list of nodes breaking the network links and nodes failing to forward the packets. The second agent keeps track of attacks and malicious behavior in the network such as forwarding the data to the wrong address or node. The two agent based trust scheme provide the network links and nodes failing to forward the packets. The second agent keeps track of attacks and malicious nodes to interconnect with the trusted nodes together which increases the level of quality of service for MANET environment[1–3]. The proposed model is tested by comparing the other trust models and the result shows that the proposed model is more efficient than any other trust models for MANET.

This paper is organized with section 2 as Trust in MANET. The section 3 describes the Agent based trust estimation model for MANET. The section 4 and 5, presents the simulation setup and result analysis. Finally, section 6 with conclusion.

2. Trust in MANET

*Author for correspondence

Trust models in MANET are proposed to provide the trust among the nodes inside cluster and outside cluster communication. In order to communicate, a large amount of private user data, preferences, behavioral habits and other information about the users are need to be processed and exchanged among various MANET nodes within the cluster and outside the cluster. With the data inferred, related conclusions will again be exchanged all over the nodes. In such environment, it is of paramount importance to assure privacy and maintain control of turbulent private information flow[4,5], whilst preventing leakages of sensitive private information. Another aspect which further blurs privacy issues is diminishing of conventional role of thin, not-trusted-user-client and large-corporate service[6,7]. Pervasive systems are service oriented platforms where everything can potentially act as a service, including the user. The opposite is also true, every service will potentially be able to take on the role of a user. In MANET environment roles of a node and service can be swapped or interchange[8,9]. These roles merely describe the nature of the communication, since the user is the party who initiates the communication and the node is the party that replies and grants access to the user. MANET systems are traditionally seen as environments where the nodes are normally not a trusted party and services are more or less trusted. Trust negotiation[10] is a process through which mutual trust is incrementally established by the gradual exchange of digital credentials and requests for credentials among entities that may have no pre-existing knowledge of each other. Digital credentials are an electronic analogue of paper credentials used to establish trust in the everyday world. Upon successful trust negotiation the supplicant is granted access to the protected resource. During trust negotiation, the disclosure of credentials is governed by access control policies. Trust negotiation has been intensely discussed in various publications in recent years[11]. The parties involved in trust negotiation will be named the supplicant and the supplier. The supplicant is the party that requests access to resource, and the supplier provides the service. Trust negotiation protocol consists of two types of messages which are exchanged between the supplicant and supplier. They are requests for credentials or resources and disclosures of resources.

3. Agent based Trust Estimation Model for MANET

The main aim of the agent based trust estimation for MANET is to provide reliable communication inside the MANET environment. The trust level of the node is estimated using two agents. The first agent keeps track of the network link failure and packet dropping, which provide the list of nodes breaking the network links and nodes failing to forward the packets. The second agent keeps track of attacks and malicious behavior in the network such as forwarding the data to the wrong address or node. The two agent based trust scheme provide the nodes to interconnect with the trusted nodes together which increases the level of quality of service for MANET environment. The trust estimation node in the environment is equipped with two agents which starts functioning whenever communication occurs in the environment. The first agent holds the constant handshakes with the cluster heads to keep track of the network link failures and the cause for the link failure. As a result first agent estimates the nodes which cause the link failure and add it to the untrusted node list. The algorithm used by the first agent to fix the node causes the link failure is shown in Figure 1.

Step 1: Packet communicates from node x in cluster p to node y in cluster q.
Step 2: Node x finds adjacent node and updates routing table up to interleaving cluster p
Step 3: Broadcast and find path for cluster q.
Step 4: Updates routing table upto cluster q.
Step 5: Broadcast and find path for node y in cluster q.
Step 6: Updates routing table upto node y in cluster q.
Step 7: Calculate time to live for packets at each node in the routing table.
Step 8: Calculate network congestion at each node in the routing table.
Step 9: Transmit packet.
Step 10: If packet is transmitted then all assign nodes in the routing table are trusted nodes.
Step 11: Else check whether link failure or packet loss due to congestion.
Step 12: If this check fails, fix the node as untrusted node and isolate from the cluster.

Figure 1. Algorithm used by the first agent to fix the node causes the link failure.

Step 1: Check for node causing link failure using first agent.
Step 2: Calculate network congestion at each node in the routing table.
Step 3: Calculate time to live for packets at each node in the routing table.
Step 4: Check for packet drop or link failure.
Step 5: Fix it as attack or malicious behavior and isolate the nod and notice to first agent.
Step 6: Check for node which makes constant network updates.
Step 7: Check the node which frequently transmits packet without handshake or route discovery.
Step 8: Fix it as attack or malicious behavior and isolate the nod and notice to first agent.

Figure 2. Algorithm used by the second agent to fix the attacks and malicious behavior in the network.

The second agent is activated after the first agent and keeps track of attacks and malicious behavior in the network such as forwarding the data to the wrong address or node. Packet dropping in the network is found by the second agent through the handshake with the cluster head and first agent to fix the attacks and malicious behavior in the network. The algorithm used by the second agent to fix the attacks and malicious behavior in the network is shown in Figure 2. Both the agents are activated to estimate the nodes trust by estimation of link break, node causing the packet loss and the node causing the attacks or malicious behavior in the network. After estimation of malicious nodes, they are fixed and isolated from the network. It is considered that other nodes are trusted nodes which will not cause any abnormality in the network. By communicating with these nodes reliable communication may be obtained.

4. Simulation Setup

The Simulation was carried out using NS/2 to check the correctness of estimation. To evaluate three environments are created. First environment was created with 50 hosts having a simulation area of 1000 x 1000 m^2 having the maximum speed of 10 meters/sec. with 250 meters as transmission range and 30 seconds as pausing time. The second environment was created with 100 hosts having a simulation area of 1500 x 1500 m^2 having the maximum speed of 10 meters/sec. with 250 meters as transmission range and 30 seconds as pausing time. The third was created environment with 500 hosts having a simulation area of 3500 x 3500 m^2 having the maximum speed of 10 meters/sec. with 250 meters as transmission range and 30 seconds as pausing time. The channel capacity of the environment is 2 Mbit/sec. with the random way point mobility model having the packet size of 512 bytes. In all the three environments 20% of the hosts are created as non trusted host, which creates malicious activity and 80% of the hosts is created as trusted hosts. The transmission was triggered from 1, 2, 5 sources in three environments respectively. 50 packets from each source are transmitted.

5. Result Analysis

Simulation results were obtained and compared with PGP Trust Model, Decentralized Trust model, Distributed Trust Model and Ant based Trust Model. The proposed model has been compared with other models with the parameters end to end delay, throughput and attacks/Errors. The results show the proposed model performed well than the existing model. The Table 1 and the Figure 3 shows the measurement of delay observed in various trust models upon which Agent Based Trust Estimation for Mobile Ad Hoc Network consumes less delay against the other trust models on all the three number of hosts with 1,2,5 sources and 50 packets transmitted from each sources.

Table 1. Delay analysis with various number of host

Model	Metric	Number of host		
		50	100	250
Agent Based Trust Estimation For Mobile Ad Hoc Network (ABTE)	Delay in Sec.	0.3	0.7	1.2
PGP Trust Model (PGPTM)		0.5	1.0	1.4
Decentralized Trust model (DZTM)		0.6	1.1	1.5
Distributed Trust Model (DTM)		0.8	1.3	1.8
Ant based Trust Model (ABTM)		07	1.0	1.3

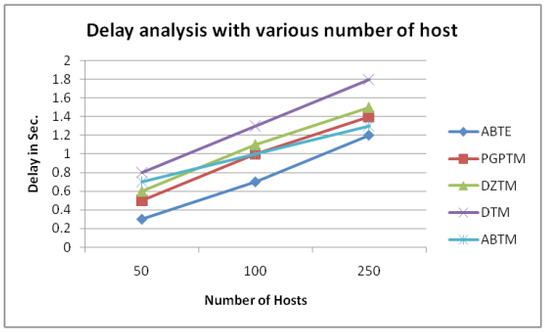

Figure 3. Delay analysis with various number of hosts.

Table 2. Throughput analysis with various number of host

Model	Metric	Number of host		
		50	100	250
Agent Based Trust Estimation For Mobile Ad Hoc Network (ABTE)	Throughput bits/ sec.	11200	9800	7800
PGP Trust Model (PGPTM)		9800	8700	7600
Decentralized Trust model (DZTM)		11000	8600	7400
Distributed Trust Model (DTM)		10800	9500	7700
Ant based Trust Model (ABTM)		10500	9300	7500

The Table 2 and the Figure 4 shows the measurement of throughput observed in various trust models upon which Agent Based Trust Estimation for Mobile Ad Hoc Network provides high throughput since the delay is low against the other trust models on all the three number of hosts with 1,2,5 sources and 50 packets transmitted from each sources. The Table 3 and the Figure 5 shows the measurement of number of attacks/errors observed in various trust models upon which Agent Based Trust Estimation for Mobile Ad Hoc Network provides low in number of attacks/errors compared with on all the three number of hosts with 1,2,5 sources and 50 packets transmitted from each sources.

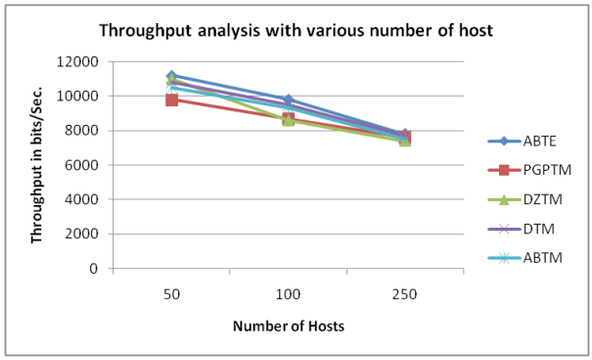

Figure 4. Throughput analysis with various number of host.

Table 3. Number of Attacks/Errors analysis with various number of host

Model	Metric	Number of host		
		50	100	250
Agent Based Trust Estimation For Mobile Ad Hoc Network (ABTE)	Number of attacks/ errors	3	12	18
PGP Trust Model (PGPTM)		7	15	28
Decentralized Trust model (DZTM)		9	18	34
Distributed Trust Model (DTM)		8	14	56
Ant based Trust Model (ABTM)		11	17	43

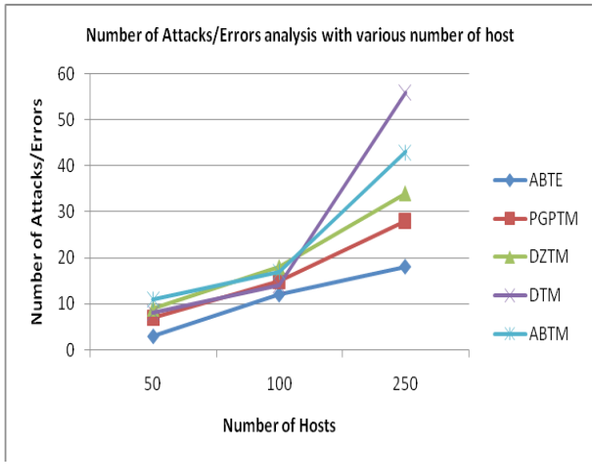

Figure 5. Number of Attacks/Errors analysis with various number of host.

6. Conclusion

To provide a reliable communication in mobile ad hoc network (MANET) communication, this paper proposed Agent based Trust estimation model. The proposed model consumes less delay and provides high through put and it also ensures number of attacks/errors is also low compared with other models.

7. References

1. Krishnan MBM, Khader PSA. Fuzzy based security model to detect compromised and selfish nodes to Mobile Ad Hoc Network. Eur J Sci Res. 2012 Sep; 86(4):520–4.
2. Krishnan MBM, Khader PSA. Trust evaluation model for mobile Ad Hoc Network. National Journal of System and Information Technology. 2011 Dec; 190–5. ISSN: 0974-3308.
3. Krishnan MBM, Khader PSA. Estimating detection trust hold for intrusion detection systems in mobile Ad Hoc Network: A comprehensive study. Journal of Computer Applications Research and Development. 2011 Apr; 1–7. ISSN: 2248-9304.
4. Krishnan MBM, Rajasekar P. Providing QoS in mobile Ad Hoc Network for multimedia communication through mining techniques. Ghaziabad, India: Proceedings of International Conference on Recent Trends in Computing (ICRTC); 2012 Oct. ISBN: 978-93-81583-67-8. p. 40–2.
5. Buttyan L, Hubaux JP. Stimulating cooperation in self-organizing mobile Ad-hoc Networks. MONET. 2003; 8(5):579–92.
6. Davis CR. A localized trust management scheme for Ad-Hoc Networks. Proceedings of the 3rd International Conference on Networking (ICN '04).
7. Eschenauer L, Gligor VD, Baras J. On trust establishment in mobile Ad-Hoc Networks. Proceedings of the Security Protocols Workshop; 2002.
8. Ghosh T, Pissinou N, Makki K. Towards designing a trusted routing solution in mobile Ad-Hoc Networks. MONET. 2005; 10(6):985–95.
9. Haripriya Y, Bindu Pavani KV, Lavanya S, Viswanatham VM. A framework for detecting malicious nodes in mobile Adhoc Network. Indian Journal of Science and Technology. 2015 Jan; 8(S2):151–5.
10. Devi U, Kaushik KV, Sreeveer B, Prasad KS. VoIP over Mobile Wi-Fi Hotspot G. Indian Journal of Science and Technology. 2015 Jan; 8(S2):195–9.
11. Helen, Arivazhagan D. Intelligent inspiration to salvage energy in Ad-Hoc Network using biological agent. Indian Journal of Science and Technology. 2014 Nov; 7(S7):51–4.