Imperial Journal of Interdisciplinary Research (IJIR)
Vol-2, Issue-5, 2016
ISSN: 2454-1362, http://www.onlinejournal.in

Trust Management in Manet

Megha Jain[1], Karan Saxena[2] & Nitin Kumar[3]
[1]Assistant Professor ,JSSATE Noida
[2,3]Student BTech IT.JSSATE Noida

Abstract: *The research looks at the works of Mario T Schlosser , Sepander D Kamvar and Hector Garcia Molina this research draws mostly form the algorithm namely Eigen trust. In this , the global reputation of each peer i is given by the local trust values assigned to peer i by other peers, weighted by the global reputations of the assigning peer. This algorithm is basically used to assign a value to every node which acts as a measure of trust worthiness and ultimately the node having the highest trust values is the node with whom the transaction of information takes place. Now adding up to this we also include the protocols like adhoc on demand vector routing and signal stability routing to perform congestion control while routing the files to the selected node according to the trust value assigned this pathway is added with a security algorithm RSA algorithm to securely transfer the file this imposed security is added keeping in mind the concepts of transmission of the right file as ensured in the torrents using seeds/peers concept I.e. the more the seeds and peers in a file more viable and better the file is.*
Mobile Ad Hoc Networks (MANETs) are an emerging type of wireless networking, in which mobile nodes associate on an extemporaneous or ad hoc basis. MANETs are both self-forming and self-healing, enabling peer-level communications between mobile nodes without reliance on centralized resources or fixed infrastructure.
These attributes enable MANETs to deliver significant benefits in virtually any scenario that includes a cadre of highly mobile users or platforms, a strong need to share IP-based information, and an environment in which fixed network infrastructure is impractical, impaired, or impossible. Key applications include disaster recovery, heavy construction, mining, transportation, defense, and special event management.

1. Introduction

The project basically focuses on implementation of cyclic trust using the adhoc network it provides an interface to the user this is basically done to ensure secure transfer of the data on the adhoc network as wireless data transmission although is a fast means but more or less it compromises on the security of the data. This project is basically developed to reap the benefits of both wireless as well as wired protocols i.e. security as well as infrastructure less networks. These benefits include security as well as faster transmission of data that too without need of any infrastructure. It's a router less mechanism thus there is a minute probability of masquerading and breaking the network. The source reliability is estimated on the basis of eigen values and the trust is estimated using the eigens value concept on each successful transmission of data eigen value of the virtually created node gets incremented thus provides reliability.

2. Second and Following Pages

The Second and following pages focusses on the basics of adhoc network followed by the implementation of trust management using the adhoc network it also shows the implementation of trust through graphs which are simulated using network simulator 2

3. Trust[4]

Managing trust in a distributed Mobile Ad Hoc Network (MANET) is challenging when collaboration or cooperation is critical to achieving mission and system goals such as reliability, availability, scalability, and configurability. In defining and managing trust in a military MANET, we must consider the interactions between the composite cognitive, social, information and communication networks, and take into account the severe resource constraints (e.g., computing power, energy, bandwidth, time), and dynamics (e.g., topology changes, node mobility, node failure, propagation channel conditions). We seek to combine the notions of "social trust" derived from social networks with "quality-of-service (QoS) trust" derived from information and communication networks to obtain a composite trust metric. We discuss the concepts and properties of trust and derive some unique characteristics of trust in MANETs, drawing upon social notions of trust. We provide a survey of trust management schemes developed for MANETs and discuss generally accepted classifications, potential attacks, performance metrics, and trust metrics in MANETs. Thus besides social activities it also helps in

managing security within various systems and hence ensuring transmission of the files to the right systems.

4. Routing Protocols

The use of routing protocols has a major role in this project as these basically helps in facilitation of congestion free packet transmission and hence it provides congestion control this is ensured by a mixture of variety of protocols like DSR(Dynamic Source Routing), AODV(Ad-hoc on demand distance vector routing) and signal stability routing. Although the most efficient transmission protocol is AODV but we use signal stability routing to ensure transmission in case the other path is not working or busy. This reduces latency and waiting time.

5. Eigen trust

The eigen trust values plays an important role in this project it marks the presence of trust as it provides a trust values to the nodes this provides reliability value of the nodes and hence the node which is found the most reliable is given the file access to run and hence this ensures trust. It can also be used widely in ecommerce websites like flip kart, snap deal wherein a user wants to purchase a particular product has been provided with the similar product suggesstion it is also used for torrents i.e. files with more seeds and peers is given better transmission bandwidths and ensured more trust worthy.

5.1. Algorithm [3]

Each peer has a number M of score managers, whose DHT coordinates are determined by applying a set of one-way secure hash functions h0, h1, . . . , hM−1 to the peer's unique identifier. posi are the coordinates of peer i in the hash space. Since each peer also acts as a score manager, it is assigned a set of daughters Di - the set contains the indexes of peers whose trust value computation is covered by the peer. As a score manager, peer i also maintains the opinion vector ci d of its daughter peer d (where d 2 Di) at some point in the algorithm. Also, peer i will learn Ai d which is the set of peers which downloaded files from its daughter peer d: It will receive trust assessments from these peers referring to its daughter peer d. Finally, peer i will get to know the set Bid which denotes the set of peers which its daughter peer d downloaded files from: Upon kicking off a global trust value computation, its daughter peer d is supposed to submit its trust assessments on other peers to its score manager, providing the score manager with Bi d.

For each *peer* i do
Submit local trust values $c\sim_i$ to all score managers at posi-tions h_m (pos_i), m = 1 . . . M − 1;
Collect local trust values $c\sim$ and sets of acquaintances B^i
d $_d$
of daughter peers $d \in D_i$;
Submit daughter d's local trust values c_{dj} to score man-agers $h_m(pos_d)$, m = 1 . . . M − 1, $\forall j \in B_d^i$;
Collect acquaintances A^i_d of daughter peers; for each *daughter peer* $d \in D_i$ do
Query all peers $j \in A^i_d$ for c_{jd} p_j ; repeat
Compute $t_d^{(k+1)} = (1 - a)(c_{1d}\, t_1^{(k)} + c_{2d}\, t_2^{(k)} + \ldots + c_{nd}\, t_n^{(k)}) + ap_d$;
Send $c_{dj}\, t_d^{(k+1)}$ to all peers $j \in B_d^i$;
Wait for all peers $j \in A^d_i$ to return c_{jd} $t_j^{(k+1)}$;
until $|t_d^{(k+1)} - t_d^{(k)}| <$.;
end end

6. Network Simulator 2

The network simulator 2(ns-2) is a compiler through which we can establish ad-hoc networks and display various parameters of network through graphical representations. we have used ns-2 in order to display the trust through graphs. Since our research focusses on circular trust management we can observe graphs showing circular patterns. In addition to trust graphs this tool is also used to represent the algorithms used like Dynamic source routing(dsr),AODV(Adhoc on demand vector routing) which are used to ensure congestion control in the system.

7.Acknowledgements

This work was supported in part by a grant from JSSATE Noida (A.K.T.U)

8.References

[1] K. Aberer and Z. Despotovic. Managing Trust in a Peer-2-Peer Information System. In *Proceedings of the 10th International Conference on Information and Knowledge Management (ACM CIKM)*, New York, USA, 2001.

[2] Captcha Project. http://www.captcha.net.

[3] Sepandar D. Kamvar Mario T. Schlosser Hector Garcia-Molina ,The EigenTrust Algorithm for Reputation Management in P2P Networks]

[4] A.Swami, I.R Chen ,J.H Cho Computational and Information Sciences Directorate, U.S. Army Research Laboratory, 2800 Powder Mill Rd., Adelphi, Maryland 20783, USA