Volume 5, Issue 6, June 2015 ISSN: 2277 128X
International Journal of Advanced Research in Computer Science and Software Engineering
Research Paper
Available online at: www.ijarcsse.com

A Comparative Study on Reliable and Unreliable Data Transfer in Mobile Adhoc Networks

Sandhya Baliga
Department of CSE
P.A.College of Engineering
Karnataka, India

Prof. Ganesh Pai
Assistant Professor, CSE
P.A.College of Engineering
Karnataka, India

Abstract*— Mobile Adhoc Networks have become a vital part of day today life. It is a network where the nodes are mobile and they configure themselves and do not require any infrastructure. Every node moves in its own way. It changes its route now and then and due to frequent movement there is partition in the network leading to disconnection of links and link failure. Congestion is also one of the problems. Use of transmission control protocol (TCP) in such networks is affected by these problems. The throughput will be extremely low. So it is not advised to use it. But use of user datagram protocol gives far worst results compared to transmission control protocol. The throughput is still low and the drop of packets is more and delivery ratio is less. Hence in this project work, we have tried to show that use of Transmission Control Protocol is better in Mobile Adhoc networks even when it gives rise to lot of problems. We have focussed on the problem of network partition and how it can be overcome by finding new alternate paths. We have also implemented a security algorithm to check that the nodes are trusted and none of them are blacklisted.

***Keywords*—Transmission Control Protocol, User Datagram Protocol, Mobile Adhoc Networks, Blacklist, Trusted**

I. INTRODUCTION

Mobile Adhoc Network is a network where the nodes are mobile which configure themselves and do not have a proper infrastructure. It is a temporary network and does not have a centralized administration. Since the routes change frequently and randomly, the topology is not known in advance. It is unpredictable at all times. A network may be broken and in a few minutes of time it might again be reformed. This is the specialty of mobile adhoc networks

Adhoc On Demand Distance Vector (AODV) routing protocol is used usually in mobile adhoc networks. This protocol is idle until a connection has to be established. Whichever node needs a connection it broadcasts an AODV Request message to other nodes. Any node that gets this message, if it has a route to that node then it replies back using that route. The routing table entries keep on recycling from time to time. If a link breaks then an error message is sent to transmitting node and this process is repeated to form the connection again.

Dynamic Source Routing (DSR) is another protocol which can be used instead of AODV. It forms a route on demand and relies on source routing strategy than using routing tables. This is to prevent updating of routing table at regular intervals and thus reduces some overhead of the protocol. It also does not use hello packets for informing other nodes that it is active.

Reliable data transfer refers to the use of Transmission Control Protocol and Unreliable data transfer refers to User Datagram Protocol. The throughput of transport protocols in mobile adhoc networks is very low compared to that of wired or fixed networks. Transmission Control Protocol is used in fixed networks which transfers data in a reliable manner increasing the throughput. But use of this protocol in mobile adhoc network leads to many problems. The problems include congestion, partition in the network, disconnection of links due to movement of nodes and many others and this leads to low throughput.

Transmission Control Protocol when used in mobile adhoc network cannot differentiate between loss of packets due to congestion and loss of packet due to other reasons. Other reasons might be loss due to partition in network or link failure or disconnection of link. So the protocol does not find much use in mobile adhoc networks. Another problem is frequent use of three way handshake for re-establishing connection among disconnected nodes.

Security is another concern here in mobile adhoc networks. Two things need to be taken care. One is enabling the nodes to establish connection securely and another is to transfer the data in a secure manner. The nodes need to be trusted and no node has to be blacklisted. It should prevent formation of loops in the networks and identify the spoofed messages and also those packets which have breach in confidentiality and integrity. There might be passive as well as active attacks. So we need to apply security and cryptographic algorithms to ensure secure data transmission. Only then a secure environment can be established in mobile adhoc networks.

In this work, we find a solution to one of the problem i.e. network partition. Whenever there is network partition, the source node finds a new route to transmit the packets so as to prevent drop of packets and improve throughput. We have compared the same procedure with user datagram protocol to show the variance in throughput. We have also implemented a security code to prove that the nodes are trusted and are not blacklisted

II. REVIEW OF LITERATURE

New techniques have been introduced for TCP New Reno in mobile ad-hoc networks for calculation of New Retransmission Time out (RTO), to improve performance in terms of congestion control. Evaluation based on comparative study of ABRA New Reno with other TCP Variants like New Reno and Reno is done using realistic parameters like TCP Packet Received, Packet Drop, Packets Retransmitted, Throughput, and Packet Delivery Ratio and these are calculated by varying attributes of Node Speed, Number of Nodes and Pause Time. Implementation and simulations are performed in QualNet 4.0 simulator [1]. The design and implementation of a TCP-friendly transport protocol has been done for ad hoc networks. They have performed multi-metric joint identification for packet and connection behaviours based on end to end measurements. Their testbed measurements and ns-2 simulations show a significant performance improvement over standard TCP in ad hoc networks [2].

An approach where a thin layer between Internet protocol and standard TCP that corrects the problems of TCP and maintains high end-to-end TCP throughput is implemented. They have implemented their protocol in FreeBSD, and have presented results from extensive experimentation done in an ad hoc network. Their solution improves TCPs throughput by a factor of 2–3[3].An NS2- based simulation analysis of TCP using omni antennas over mobile ad-hoc network is conducted. They have compared the performance of end to end protocols such as TCP-New reno and TCP-SACK with the routing provided by AODV, DSR and DSDV protocols using omni directional antenna [4].

The effects that link breakage due to mobility has on TCP performance are found. Through simulation, it is shown that TCP throughput drops significantly when nodes move, due to TCP's inability to recognize the difference between link failure and congestion. It is shown how the use of explicit link failure notification (ELFN) techniques can significantly improve TCP performance [5]. A new approach to improve TCP performance by detecting and responding to out-of-order packet delivery events, which are the results of frequent route changes, is found. This approach had achieved on average 50% performance improvement, without requiring feedback from the network or the lower layer[6].

TCP may perform very bad in mobile adhoc networks and provides a quantitative characterization of this performance gap. Their findings indicate that node mobility, especially mobility-induced network disconnection and reconnection events, has the most significant impact on TCP performance. They have found that TCP New Reno merely achieves about 10% of a reference TCP's throughput in such cases. As mobility increases, the relative throughput drop ranges from almost 0% in static case to 1000% in highly mobile scenario (mobility speed is 20m/sec). In contrast, congestion and mild channel error (say, 1%) have less visible effect on TCP [7]. It is shown how TCP can be affected by mobility and lower layers protocols. In addition, it is surveyed at the main proposals which aim at adapting TCP to mobile and static Ad hoc environments [8].

Use of public key cryptosystems for security is common in mobile adhoc networks and sensor networks and a survey has been carried out to find percentage of its efficiency [9][10]. Use of certificates has been a trend in public key cryptography. But this paper suggests the absence of certificates to maintain security in mobile adhoc networks. Also a secret method of sharing key is used among few nodes and any attacks on them is identified [11].Key distribution using cluster head has been introduced leading to better security in mobile adhoc networks [12].Different methods of key distribution is specified so as to efficiently transfer the key among the parties [13][14].Many papers have shown the statistics of TCP and its variants in mobile adhoc network with plot of graph of different parameters versus time.[15][16][17][18].

III. EXISTING SYSTEM

There are several methods to improve throughput in mobile adhoc networks. The variants of Transmission Control Protocol like TCP Reno, TCP New Reno, and TCP Vegas are implemented. Introduction of a new intermediate layer between Transmission Control Protocol and Internet Protocol have improved the throughput to a major extent. Use of messages like Explicit Congestion Control and Destination Unreachable to indicate congestion and network partition problems have been implemented. Methods which implement recalculation of retransmission timeout have been used. Several cryptosystems have been used to check for trust and blacklisting. Different methods of sharing keys and distribution are utilized. Use of public key cryptosystems for security has been implemented in mobile adhoc networks and sensor networks. Use of certificates has been a trend in public key cryptography. The absence of certificates to maintain security in mobile adhoc networks has also been conducted. Also systems with secret method of sharing key is used among few nodes have been implemented and any attacks on them will be identified through it.

IV. PROPOSED SYSTEM

We have tried to compare the usage of Transmission Control Protocol and User Datagram Protocol. When there is network partition we find a new route to destination node from the source and check throughput and other metrics like delivery ratio, number of transmitted, received and dropped packets. It is compared with use of User Datagram Protocol for better efficiency. We have also implemented a security code that verifies that all nodes including source and destination are trusted for communication and are not blacklisted. In case they are, the code gives you a warning to proceed with communication without any security.

A. Simulation Setup

Simulation is used to implement the system. We are using NS-2 for this.NS-2 simulation is carried out by writing the tcl code. This tcl coding is simple and easy to learn and write code. Knowledge of basic syntax is sufficient to code. Some parameters need to be initialised at the beginning like the channel, radio propagation model, queue interface and size, network interface type, routing protocol etc.

set val(chan) Channel/Wireless Channel
set val (prop) Propagation/TwoRayGround
set val(netif) Phy/WirelessPhy
set val(ifqlen) 50
set val(rp) AODV
set val(ifq) Queue/Drop Tail/PriQueue

B. Modules

- *Create nodes and network topology.*
- *Static routing table and transfer of packets*
- *Security code to check if the nodes are trusted and not blacklisted.*
- *Find throughput and other network parameters*

i) Create nodes and network topology

We built the topology of N different nodes and give initial movements to it in order to give the feel of mobile adhoc networks. Two nodes are marked as source and destination nodes for packet transfer.

ii) Static routing table and transfer of packets

A static routing table is designed for the mobile adhoc network which is used in the creation of clusters. Code for efficient packet delivery is written. In case there is network partition, in order to avoid drop of packets the source finds a new route to the destination. After network partition occurs we assume that the source is intimated about it following which a new path is established. Network partition occurs when a node moves away from another node's range which is transferring data leading to link breakage and drop of packets.

iii) Security code to check if the nodes are trusted and not blacklisted.

Before the transfer of packets, a security code is executed to find the presence of trusted and non blacklisted nodes. If all nodes are trusted and non blacklisted then only the data transfer is said to be secure else a warning is issued before the packet transfer. In order to find trust, we divide the network topology into clusters. We use the routing table details to do this. We select the node with highest weight or the one with maximum neighbours as the first cluster head and include its neighbours in the cluster. Next iteration we exclude these nodes and again select node with next highest weight and the procedure is continued. Once clusters are formed, all nodes will generate their self certificates and send it to their respective cluster heads. Whenever we have to transfer data, the cluster heads of source and destination nodes will exchange the certificates and each one will also get the self certificate from the sender or receiver nodes and compare both the certificates. If both are same they are trusted. Other nodes having at least one neighbour is considered as trusted and not blacklisted. Even if one node is untrusted or blacklisted the system issues a warning that communication is insecure.

iv) Find throughput and other network parameters.

Throughput, delivery ratio, transmitted, received and dropped packets for Transmission Control Protocol and User Datagram Protocol is found and compared for better efficiency in mobile adhoc networks during network partition.

C. Algorithm For the System

Step 1: Create the network topology with N nodes.
Step 2: Initialise the simulation parameters and movements of nodes.
Step 3: Create a static routing table.
Step 4: Check if the nodes are trusted and not blacklisted. For this, clusters are created and certificates are generated and sent to cluster head. The cluster heads of source and destination exchange the certificates and compare with the certificate obtained from node directly. If any node is not trusted it gives a warning about insecure communication before packet transfer.
Step 5: While sending packets from source to destination, if network partition occurs in the selected path then source should be notified and source should find a new path for packet transfer.
Step 6: Run the same simulation for Transmission Control Protocol and User Datagram Protocol.
Step 7: Find the throughput and other network parameters to find which protocol works better in mobile adhoc networks.

V. RESULTS AND DISCUSSION

We have created a network topology of 15 nodes and given initial movement to the nodes. While executing the system, we have found that no nodes are untrusted or blacklisted since our routing table had nodes with each one having neighbours. Hence the simulation executes as the communication is secure. Transmission Control Protocol shows throughput twice than that of User datagram protocol. The number of packets dropped will be high in case of datagram delivery. The end to end delay is almost the same. Following are detailed results. Note that the simulation is run for 70 ms.

Table I: Comparison of Reliable and Unreliable data transfer

	Transmission Control Protocol	User Datagram Protocol

Throughput	714.46 kbps	352.61kbps
End to End Delay	6.62 ms	7.96 ms
Packet delivery ratio	99.95%	98.5%
Transmitted Packets	12436	6304
Received Packets	12431	6214
Dropped Packets	5	89

VI. CONCLUSION

Mobile adhoc networks have become an integral part of future networks. Hence it has been made secure and free from problems which reduce its throughput. This system makes an attempt to show that though use of Transmission Control Protocol leads to a number of problems, when compared to other protocols its throughput is high and drop of packets is less. It allows secure communication between the nodes.

REFERENCES

[1] Dhananjay Bisen and Sanjeev Sharma School Of Information Technology, RGPV, BHOPAL, INDIA," IMPROVE PERFORMANCE OF TCP NEW RENO OVER MOBILE AD-HOC NETWORK USING ABRA", International Journal of Wireless & Mobile Networks (IJWMN) Vol. 3, No. 2, April 2011.

[2] Zhenghua Fu, Benjamin Greenstein, Xiaoqiao Meng, Songwu Lu Computer Science Department, University of California, Los Angeles," Design and Implementation of a TCP-Friendly Transport Protocol for Ad Hoc Wireless Networks", 10 th IEEE International Conference on Network Protocols (ICNP'02).

[3] Jian Liu, Member, IEEE, and Suresh Singh, Member, IEEE," ATCP: TCP for Mobile Ad Hoc Networks", IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS, VOL. 19, NO. 7, JULY 2001.

[4] K.Kathiravan ,B S Abdur Rehman Crescent Engineering College Vandalur, Chennai and Dr. S. Thamarai Selvi Professor MIT Chromepet Campus Anna University, Chennai and A.Selvam BSA Crescent Engineering College Vandalur, Chennai," TCP PERFORMANCE ANALYSIS FOR MOBILE AD HOC NETWORK USING ON- DEMAND ROUTING PROTOCOLS", www.ubicc.org, Volume 2 Number 2.

[5] GAVIN HOLLAND,Department of Computer Science, Texas A&M University, College Station, USA and NITIN VAIDYA,Department of Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, Urbana,USA," Analysis of TCP Performance over Mobile Ad Hoc Networks", Wireless Networks 8, 275–288, 2002.

[6] Feng Wang,Department of Computer Sciences,The University of Texas at Austin and Yongguang Zhang,HRL Laboratories, LLC,Malibu, California, "Improving TCP Performance over Mobile AdHoc Networks with Out of Order Detection and Response", MOBIHOC'02, June 911, 2002, EPFL Lausanne, Switzerland.

[7] Zhenghua Fu, Xiaoqiao Meng, Songwu Lu UCLA Computer Science Department, Los Angeles," How Bad TCP Can Perform In Mobile Ad Hoc Networks", Seventh International Symposium on Computers and Communications (ISCC'02) 1530-1346/02.

[8] Ahmad Al Hanbali, Eitan Altman, Philippe Nain INRI,Sophia Antipolis Cedex, France," A Survey of TCP over Ad Hoc Networks".

[9] F. Amin, A. H. Jahangir, and H. Rasifard, "Analysis of Public-Key Cryptography for Wireless Sensor Networks Security", World Academy of Science, Engineering and Technology 41, 2008.

[10] J. Chen and J. Wu, "A Survey on Cryptography Applied to Secure Mobile Ad Hoc Networks and Wireless Sensor Networks" to appear in Handbook of Research on Developments and Trends in Wireless Sensor Networks: From Principle to Practice, H. Jin and W. Jiang (eds), IGI Global, 2010.

[11] Y. Zhang, W. Liu, W. Lou, Y. Fang, and Y. Kwon, "AC-PKI: Anonymous and certificateless public-key infrastructure for mobile ad hoc networks," in IEEE ICC'05, Seoul, Korea, May 2005.

[12] K. H. Rhee, Y. H. Park, and G. Tsudik, "An Architecture for Key Management in Hierarchical Mobile Ad-hoc Networks," J. Commun. and Networks, vol. 6, no. 2, June 2004, pp. 156–62.

[13] G. Hadjichristofi, W. Adams, and N. Davis, "A Framework for Key Management in Mobile Ad Hoc Networks", International Conference on Information Technology: Coding and Computing (ITCC'05) - Volume II, 2005, pp. 568-573.

[14] Nen-Chung Wang , Shian-Zhang Fang , "A hierarchical key management scheme for secure group communications in mobile ad hoc networks", Science Direct, The Journal of Systems and Software 2007.

[15] Yuvaraju B N, Dr. Niranjan N Chiplunkar "Scenario Based Performance Analysis of Variants of TCP Using NS2-Simulator" International Journal of Computer Aplications, Vol. 4(9), 2010.

[16] Rajneesh Kumar, Sandhya Umrao "Performance based Reliable Data Communication Analysis on TCP, UDP by varying nodes, mobility speed and zone radius over ZRP" International Journal of Engineering Research and Applications (IJERA), pp. 34-39, March 2014.

[17] H. Balakrishnan, V. Padmanabhan, S. Seshan, and R. Katz, "A comparison of mechanisms for improving TCP performance over wireless links," IEEE Transactions on Networking, vol. 5, no. 6, pp. 756–769, Dec. 1997.

[18] V. Anantharaman, S. J. Park, K. Sundaresan, and R. Sivakumar, "TCP performance over mobile ad hoc networks: A quantitative study," Journal of Wireless Communications and Mobile Computing, vol. 4, no. 2, pp. 203–222, Mar. 2004.

[19] Tarasov. M, Seitz. J., Artemenko.O.,"A network partitioning recovery process in Mobile Ad-Hoc Networks", Wireless and Mobile Computing, Networking and Communications (WiMob), 2011 IEEE 7th International Conference.

