ISSN: 0976-3104
SPECIAL ISSUE: (Emerging Technologies in Networking and Security (ETNS)

ARTICLE OPEN ACCESS

A REVIEW ON EFFECTIVE TRANSFER OF DATA PACKETS USING MULTICAST ALGORITHM

SN Ranjini*, AS Renugadevi, P Brindha
Dept. of Computer Science and Engineering, Vivekanandha College of Engineering for Women, Elayampalayam, Tamilnadu, INDIA

ABSTRACT

This paper deals with the secure routing with multicast algorithm. To increase the lifetime of network, a key design factor is being improved. Because of this increased network lifetime, power metrics of the neighboring node table, routing table and group table can be improved. The data transfer can be done in an effective way by storing the neighboring nodes information within a particular network and the routes information which is useful in transferring the data from one node to the other without congestion. By using the routing information, expire time of the data packets can be known.

Published on: 2nd -December-2016

KEY WORDS

transfer of data packets, multicast routing.

***Corresponding author: Email:** ranjiniramesh177@gmail.com; **Tel.:** +91 8220624546

INTRODUCTION

Wireless sensor networks are the emerging technique which is mainly nowadays useful to transfer the data packets in the form of sound, light, etc. through a waveguide of air medium. The main impact of this paper is to deal with incorporating the multicast algorithm within a network to increase the lifetime and congestion free transmission of data packets to the destined address. The objective of the WSN is to collect specific data and send it to the required destination. WSNs were studied for many purposes, but research is now focused on a wide range of consumer industries, giving rise to the notion of ubiquitous computing.

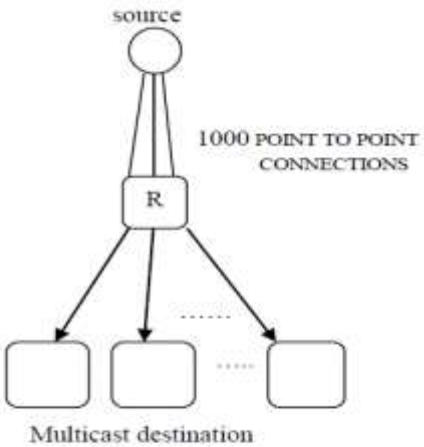

Fig.1a

………

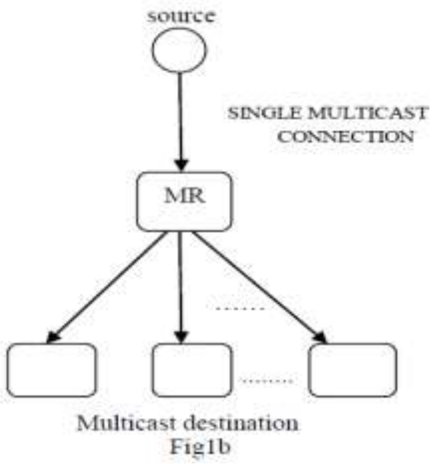

Fig1b

……

Multicasting is the ability of a communication network to accept a one message from an application and to release copies of the message to many recipients at alternate locations. One of the challenges is to reduce the amount of network resources employed by multicasting. To illustrate this point, assume that a video server wants to transmit a movie to 1000 recipients **[Figure- la]**. If the server were to employ 1000 divide point-to-point connections (e.g., TCP connections), 1000 copies of the movie may have to be sent over a single link, thus making poor use of the available bandwidth. An efficient implementation of multicasting permits much better use of the available bandwidth by transmitting at most one copy of the movie on catch link in the network, as shown in**[Figure- lb]**. Recently, there has been a lot of research in the area of multicast communication.

LITERATURE SURVEY

Over the years, there have been several methods in enhancing the technique of data transfer through different techniques. Initially, separate technique is being used to increase the speed of data transfer without any conflict in achieving the data at the destination point. For example, distance vector routing is being used to find the distance between the source node and destination node. This algorithm can find only the routing distance. But nowadays, several techniques are being implemented as a package where all the details can be utilized at a time. Ad Hoc is the wireless technique which uses the secure transfer of data. As there are limited resources in MANET so it faces many problems such as security, limited bandwidth, range and power constraints. Due to this, many new routing protocols are proposed.

The Distributed Multipath Routing Protocol for hybrid wireless networks which establishes multiple paths between source and destination. Reveal the efficient use of watchdog technique in existing trust systems, and propose a suite of optimization methods to minimize the energy cost of watchdog usage, while keeping the system's security in a sufficient level. It reduces overhead and path loss. It also has a congestion control algorithm to avoid traffic among the base stations.

Clustering is a technique which is more effective to exalt system performance. SET IBS and SET IBOOS are two Secure and efficient data transmission protocol for cluster based WSNs. They are used Identity Based digital Signature (IBS) method and Identity Based Online/Offline digital Signature (IBOOS) methods, where the clusters are formed dynamically and periodically.

Even though SET IBS and SET IBOOS are secured routing protocols, it has some demerits like energy efficiency, trustability and elongating network lifetime. To overcome these issues, Reliable Minimum Energy Cost Routing (RMECR) and Reliable Minimum Energy Routing (RMER) are two routing algorithms proposed for Mobile Ad-hoc network in which trustability is ensured either hop by hop or end to end retransmissions. It considers the energy level in a battery of a node and also through send a links to find energy efficient and trustable paths that improves the working longevity of the network

MANETs require privacy and communication security in routing protocol. In this paper present the type of attacks and operation on network layer with routing protocol technique i.e. based on an on-demand location based on anonymous MANET routing protocol called SMRT (secure MANET routing technique) with trust model that achieves security and privacy against insider and outsider adversaries.

In [1], "ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks", authors “Yuxin Liu, Mianxiong Dong, Kaoru Ota and Anfeng Liu”, A review describes the High successful routing probability, security and scalability. The ActiveTrust scheme can quickly detect the nodal trust and then avoid suspicious nodes to quickly achieve a nearly 100% successful routing probability.

In [2], "Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks", authors “M.Pushpalatha, Revathi Venkataraman, and T. Ramarao”, explain the High energy efficiency. The ActiveTrust scheme fully uses residue energy to construct multiple detection routes.

In [3], "A Reputation-based Trust Management System for P2P Networks", authors “Ali Aydin Selcuk, Ersin Uzun and Mark Resat Pariente”, says the simple and efficient in design and can be integrated into most first generation P2P systems easily. A diverse set of simulation experiments conducted to test the performance of the system exhibit that it can be highly effective in preventing the spread of malicious content.

In [4], "Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol", authors “Dr.Aditya Goel and Ajaii Sharma”, describes the mobility bahaviour has ben controlled by the approach Optimized-AODV Protocol, it uses the ant colony optimisation algorithm. They have increased the lifetime of the network, by the means of discovering new shortest routes from path accumulation. This method entirely depend upon artificial intelligence algorithms like ACO, to find the best routes which may result into high process and load on the device. This difficulty in this approach, affect the performance of the system.

In [5], "A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks", authors “Chonggun Kim, Elmurod Talipov and Byoungchul Ahn”, explains the reverse AODV method has been used. It tries multiple route replies when compare to AODV protocol. The main motto of this work is to reduce the communication delay and power consumption, but this have given efficiency in reduces path fail correction message.

In [6],"Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2", authors “Asma Tuteja, Rajneesh Gujral and Sunil Thalia”, describes the comparative performance has been done for Mobile Ad-Hoc network routing protocols like DSDV, AODV and DSR. This paper deals only about the improvement throughput, End to End Delay, Routing overhead, Packet Delivery Ratio and network lifetime. Eventhough the network lifetime is not increased up to the mark.

In [7],"Trust management in mobile ad hoc networks for bias minimization and application performance maximization", authors “Ing-Ray Chen, Jia Guo, Fenye Bao and Jin-Hee Cho”, describes the effectiveness of proposed approach with an integrated social and quality-of-service (QoS) trust protocol (called SQTrust) with which we identify the splendid trust aggregation setting under which trust bias is minimized despite the presence of malicious nodes performing slandering attacks.

In [8], “Trust Based Routing in Mobile Ad-Hoc Networks”, authors “Vinesh H. Patel, Mukesh A. Zaveri, and Hemant Kumar Rath”, explains the Routing protocols are vulnerable to routing attacks like packet dropping and delayed packet forwarding. The proposed scheme is implemented in QualNet simulator with modification in the AODV routing protocol by incorporating the trust model based approach increase network lifetime and improves network performance in presence of malicious activities.

In [9], “A Light-Weight Trust based Mobility Aware Routing Algorithm for Mobile Ad Hoc Networks”, authors “Saurin J. Choksi and Nikhil N. Gondaliya”, explains the applying security the packet forwarding behaviour of the nodes is used and for mobility speed and the relative direction of the node is taken. The algorithm is implemented on AODV protocol and checked the final simulation results against the normal AODV and trust based AODV (that uses only forwarding behaviour of the nodes) using NS2.

In [10], “Mobile Target Detection in Wireless Sensor Networks With Adjustable Sensing Frequency”, authors “Yanling Hu, Mianxiong Dong”, Kaoru Ota, Anfeng Liu and Minyi Guo, describes the important issue of the

THE IIOAB JOURNAL ISSN: 0976-3104

balance between the quality of target detection and lifetime in wireless sensor networks. Two target-monitoring schemes are proposed. One scheme is Target Detection with Sensing Frequency K (TDSFK), which distributes the sensing time that currently is only on a portion of the sensing period into the whole sensing period. That is, the sensing frequency increases from 1 to K. The other scheme is Target Detection with Adjustable Sensing Frequency (TDASF), which adjust the sensing frequency on those nodes that have residual energy.

COMPARITIVE ANALYSIS

S.No	Title	Techniques	Advantages	Disadvantages
1	Load-balancing in MANET shortest-path routing protocols	Multipath Routing Protocol	-Multi-path routing can balance the load better than single-path routing, only if we use a very large number of paths between any source-destination pair of nodes.	-No secret share from the source to destination. -Security issue on multipath routing protocol.
2	An Efficient Countermeasure to the Selective Forwarding Attack in Wireless Sensor Networks	multi-path DSR	-The multi-Path topologies (DSR) scheme to defend against the selective forwarding Attack. -The DSR scheme has some advantages. -First, the base station can receive information sensing from sensor nodes continuously under the selective forwarding attack. Second, this scheme is lightweight and simple. -Third, the dropped packets do not need to be re-sent when detecting malicious sensor nodes. Finally, this scheme can defend several kinds of attacks.	-The communication distance can be Increased and waste of communication cost. -It's seriously affect the network lifetime.
3.	H-SPREAD: A Hybrid Multipath Scheme for Secure and Reliable Data Collection in Wireless Sensor Networks.	SPREAD	-The advantage of this algorithm is that through multi-path routing, each path routes only one share, and the attacker must capture at least *T* shares to restore nodal information, which increases the attack difficulty.	-This mechanism will improve both reliability and security at the same time. -This weakness opens the door for various attacks if the routing algorithm.
4.	A Reliability-Oriented Transmission Service in Wireless Sensor Networks	proliferation routing capability-based path finder, randomized disparity, and reproduction	-The basic idea is that we estimate the packet loss in a several-hop manner and generate new packet copies after certain steps. -The packet loss and packet generation so that the E2E service quality can be maintained with any length of the data paths and the scale of the network.	-the energy efficiency of proliferation routing is not encouraging yet. -The capability-based path finder only works for transmission from sensors to sink. For general communications, say sensor-to-sensor, more investigations are needed.
5.	Design and Implementation of TARF: A Trust–Aware Routing Framework WSN's	Trust-aware routing framework protocol (TARF)	-A robust trust-aware routing framework for dynamic WSNs. Without tight time synchronization or known geographic information, TARF provides trustworthy and energy-efficient route. -Using trust and energy cost for route decisions, to prevent malicious nodes from misleading network traffic	-This approach affect network lifetime. -Affects system performance. The trust route mechanism has high costs and is difficult to obtain trust, so the guiding significance is limited
6	Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol	AODV Protocol	-Two important mechanisms, Route Discovery and Route Maintenance. -AODV is chosen for the obvious reason that it is simple and has a low overhead and its on-demand nature does not unduly burden the networks.	- It is designed to be self-starting in an environment of mobile nodes, withstanding a variety of network behaviors such as node mobility, link failures and packet losses.
7	DSDV Routing	DSDV protocol	-In proactive protocols, routes to all	-This increases the overhead

	Protocols in MANET using NS2		the nodes in the network are discovered in advance. - broadcasts after a fixed interval of time independent of any route changes or not.	and so decreases the throughput of network using DSDV protocol. In DSDV Protocol, every node stores one or more routing tables.
8	AODV Routing Protocols in MANET using NS2	AODV protocol	Reactive protocol as AODV protocol.	-AODV only stores address of next hop to the destination. -It is a reactive protocol as it only requests a route when needed and does not require nodes to maintain routes to the destinations that are not actively used in communication.
9	DSR Routing Protocols in MANET using NS2	DSR protocol	-DSR (Dynamic Source Routing) is a source initiated. -It stores complete route from source to destination including all the intermediate nodes.	-Sender of the packet determines the complete sequence of nodes through which to forward the packets; the sender explicitly lists this route in the packet's header, identifying each forwarding "hop" by the address of the next node to which to transmit the packet on its way to the destination host.
10	A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks	R-AODV Routing protocol	to avoid RREP loss - improve the performance of routing in MANET. - R-AODV prevents a large number of retransmissions of route request messages, and diminishes the congestion in the network.	RREP Delivery Fail

PROPOSED SYSTEM

This paper aims at using the technique of multicast algorithm. In this algorithm, three main properties have been included to improve the power aware metrics and congestion free routing. The information of neighboring node is helpful in transferring the data packets to the destined point with the destination address. The group name as well as address of the data packets of any particular network is provided in the group node. The details of the neighboring node and routes are provided in the neighboring node and routing table. By using all these information, the data can be sent to the required destination point in a faster manner.

RESULT AND DISCUSSION

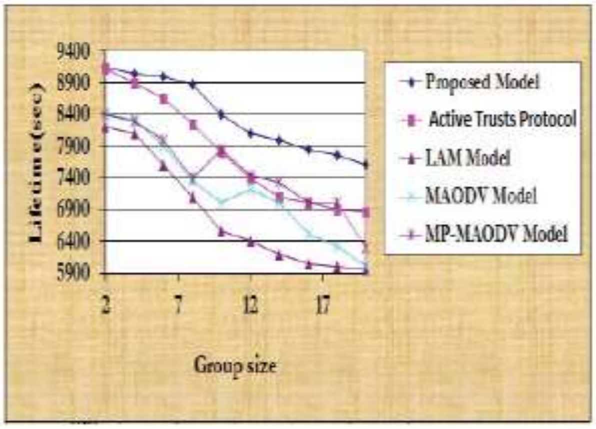

Fig. 2: Group size node versus lifetime

ISSN: 0976-3104

The proposed system and along with the protocols like Active Trust protocol, LAM Model, MAODV model, MP-MAODV has been simulated to show the performance of time along with the group size of wireless nodes. It is clear from the simulated result that the network lifetime is increased for the proposed system when compare to all other methods. During the initial stage, the value starts at 9000sec, for a group size of 2. The power sources have a very low negative gradient during the initial stages, and reach the value of 8900sec at group size 7. Then after that if the groups size has been increasing, the network lifetime decreasing steadily, and it reaches the saturation level of 7500sec for group size greater then 17, but for other networks the value reached around 5900sec.

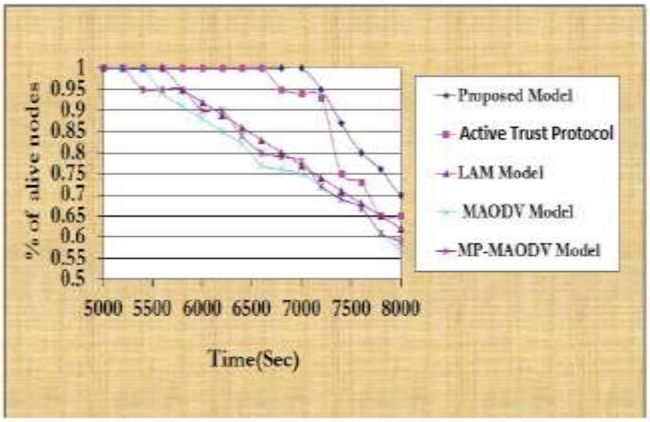

Fig. 3: Time against percentage of alive-nodes

The next parameter shows the characteristics curve of percentage of alive nodes along with time. Even in this parameter too, the proposed method excels the other existing methods. Till 7000sec, all nodes are alive, it begin to decrease at after 7000sec, and reaches 75% at 8000sec.

From the both performance curve, it shows the proposed system performs better than the all other existing system. If we incorporate this technique, we will have increase in lifetime of the nodes. This proposed system mainly deals with the secure transmission of data packets to the destination point of multiple recipients in a particular network. This transmission should be secure and congestion free technique.

CONCLUSION

This whole paper mainly focuses on delivery of data packets to multiple users with the help of multicast algorithm. This technique also utilizes the node configuration for the secure transmission through wireless sensor network. The Ad Hoc is also one of the method to transfer the data. Some of the disadvantages are faced in that technique mainly the security of data transfer. But in this proposed system encryption is done with in that particular network. Moreover , in this technique the neighboring node details as well as distance and expire time are well known. The main advantage of this system is the increment of network lifetime.

CONFLICT OF INTEREST

The authors declare no conflict of interests.

ACKNOWLEDGEMENT

None

FINANCIAL DISCLOSURE

None

REFERENCES

[1] Yuxin Liu, Mianxiong Dong, Kaoru Ota and Anfeng Liu.[2016] ActiveTrust: Secure and Trustable Routing in Wireless Sensor Networks, IEEE Transactions on Information Forensics and Security,11(9)

[2] M. Pushpalatha, Revathi Venkataraman, and T Ramarao.[2009] Trust Based Energy Aware Reliable Reactive Protocol in Mobile Ad Hoc Networks. *International Journal of Electrical, Computer, Energetic, Electronic and Communication Engineering*, 3(8): 1535-1538.

ISSN: 0976-3104

[3] Ali Aydin Selcuk, Ersin Uzun and Mark Resat Pariente.[2008] A Reputation-based Trust Management System for P2P Networks, International Journal of Network Security, 6(3):235-245

[4] Aditya Goel, Ajaii Sharma. Performance Analysis of Mobile Ad-hoc Network Using AODV Protocol", *International Journal of Computer Science and Security (IJCSS),* 3(5): 334-343.

[5] Chonggun Kim, Elmurod Talipov and Byoungchul Ahn.[2006] A Reverse AODV Routing Protocol in Ad Hoc Mobile Networks, IFIP International Federation for Information Processing ,EUC Workshops, LNCS 4097, pp. 522 – 531,

[6] Asma Tuteja, Rajneesh Gujral and Sunil Thalia.[2010]Comparative Performance Analysis of DSDV, AODV and DSR Routing Protocols in MANET using NS2, 2010 International Conference on Advances in Computer Engineering, pp 330-333

[7] Ing-Ray Chen, Jia Guo, Fenye Bao, Jin-Hee Cho, "Trust management in mobile ad hoc networks for bias minimization and application performance maximization", Adhoc Networks, Elseiver, 19: 59-74 , 2014.

[8] Vinesh H Patel, Mukesh A Zaveri, and Hemant Kumar Rath.[2015] Trust Based Routing in Mobile Ad-Hoc Networks, Lecture Notes on Software Engineering, 3(4) November 2015.

[9] Saurin J Choksi, Nikhil N Gondaliya, [2014] A Light-Weight Trust based Mobility Aware Routing Algorithm for Mobile Ad Hoc Networks", International Journal of Computer Applications, 97(14).

[10] Yanling Hu, Mianxiong Dong, Kaoru Ota, Anfeng Liu and Minyi Guo, "Mobile Target Detection in Wireless Sensor Networks With Adjustable Sensing Frequency, *IEEE systems journal*.

[11] Mianxiong Dong, Kaoru Ota, Anfeng Liu and Minyi Guo, Joint Optimization of Lifetime and Transport Delay under Reliability Constraint Wireless Sensor Networks, *IEEE transactions on parallel and distributed systems*, tpds-2013-12-1250.

[12] Shibo He, Jiming Chen, Fachang Jiang, David KY Yau, Guoliang Xing and Youxian Sun.[2013] Energy Provisioning in Wireless Rechargeable Sensor Networks, *IEEE transactions on mobile computin*g, 12(10)

[13] Chunsheng Zhu, Hasen Nicanfar, Victor CM Leung, Laurence T Yang. [2014]An Authenticated Trust and Reputation Calculation and Management System for Cloud and Sensor Networks Integration, IEEE transactions on information forensics and security,

[14] Zhongming Zheng, Anfeng Liu, Lin X Cai, Zhigang Chen, and Xuemin (Sherman) Shen, "Energy and Memory Efficient Clone Detection in Wireless Sensor Networks, 10.1109/TMC.2015.2449847, IEEE Transactions on Mobile Computing.

[15] C Rajan, N Shanthi.[2015] Genetic based Optimization for multicast Routing algorithm for Manet' Sadhana - Academy Proceedings in Engineering Science, 40(7): 2341-2352.

[16] Shigen Shen, Hongjie Li, Risheng Han, Athanasios V. Vasilakos, Yihan Wang, Qiying Cao.[2014] Differential Game-Based Strategies for Preventing Malware Propagation in Wireless Sensor Networks, IEEE transactions on information forensics and security, 9(11).

ABOUT AUTHORS

S.N. Ranjini : *Graduate student, Department of Computer Science and Engineering, Vivekanandha college of engineering for women, Elayampalayam Tamilnadu, India*

A.S. Renugadevi *: Assistant Professor, Department of Computer Science and Engineering, Vivekanandha college of engineering for women, Elayampalayam Tamilnadu, India*

P. Brindha *: Assistant Professor, Department of Computer Science and Engineering, Vivekanandha college of engineering for women, Elayampalayam Tamilnadu, India*