ISSN: 2321-9653

INTERNATIONAL JOURNAL FOR RESEARCH IN APPLIED SCIENCE AND ENGINEERING TECHNOLOGY (IJRASET)

Improve Efficiency Of Data Brodcasting In Wireless Network

Umesh Pandey[1], Sushil Ku.Kashyap[2], Dr.S.K.Shrivastava[3]

[1]*DR.C.V.RAMAN UNIVERSITY, BILASPUR, INDIA,*
MPHIL SCHOLAR

[2]*Dr.C.V.RAMAN UNIVERSITY, BILASPUR, INDIA,*
PHD SCHOLAR

PROFESSOR
[3]*RAJEEV GANDHI GOVT.P.G.COLLEGE, AMBIKAPUR (SURGUJA)*

Abstract: the wireless ad hoc networks and we proposed an algorithm for Proficient Data Broadcast Technique which is help full for reducing data replica as well as try to improve the overall performance of the network. on the other hand we have seen that Wireless Network are highly vulnerable to attacks due to their characteristics that have been discussed in this thesis. The research work that has been done to secure the Wireless Networks and various background concepts related to our work are also studied. An adhoc network is a collection of wireless mobile hosts forming a temporary network without the aid of any centralized administration or standard support services regularly available on the wide area network to which the host may normally be connected". Since the nodes are highly mobile, the network topology changes frequently and the nodes are dynamically connected in a arbitrary manner. Further, the limitation imposed on the transmission range of the nodes have lead to the development of routing policy where packets are allowed to traverse through multiple nodes thus making each node act as terminal as well as router. Since the nodes in adhoc networks are free to move over a certain area which results into frequent change in the network topology, design of suitable routing protocol is essential to adapt the dynamic behavior of the network.

Keywords: adhoc network, Vector Routing, nodes mobile. Wireless transmission, Efficient Data Broadcasting

I.INTRODUCTION

In recent years, In the last few years, we have seen the rapid development of wireless communication technologies. Today wireless technologies are widely used across the globe to maintain the communication needs of a huge number of end users [1]. A Wireless network is a collection of wireless mobile nodes energetically forming a temporary network without the use of presented network infrastructure or centralized administration. Wireless Networks have developed into a hot topic in research. Their capabilities for monitoring large areas, accessing remote places, real-time reacting, and relative ease of use has brought scientists a whole new horizon of possibilities [2,3].Due to the partial transmission range of wireless network interfaces, multiple network hops may be needed for one node to replace data with another across the network. In such a network, each movable node operates not only as a host but also as a router, forwarding packets for other movable nodes in the network, that may not be within the direct achieve a wireless transmission range of each other[4]. Each node participates in an ad hoc routing protocol that allows it to determine multi hop paths through the network to any other node.

Adhoc On-Demand Distance-Vector Routing Protocol (AODV)

AODV is an on-demand routing protocol that has been developed specially for MANET. In AODV whenever a node

IJRASET: ISSN: 2321-9653

needs to send data to another node that it does not have a route to it tries to discover a new route. The route discovery process is initiated by the route request (RREQ) message. The source node floods the RREQ packet in the network when a route is not available for the desired destination [5]. A RREQ carries the source IP address, the destination IP address, the source sequence number, the destination sequence number, the broadcast identifier and the time to live (TTL) field. The wireless network has so far been employed in military activities such as reconnaissance, surveillance, and target acquisition, environmental activities such as forest fire prevention, or civil engineering such as structural health measurement. Their uses increase by the day and their potential applications seem boundless [6]. The wide variety of applications results in a wide variety of networks bearing different constraints and having different features, yet most of these networks share some common issues that allow them to be treated homogeneously.

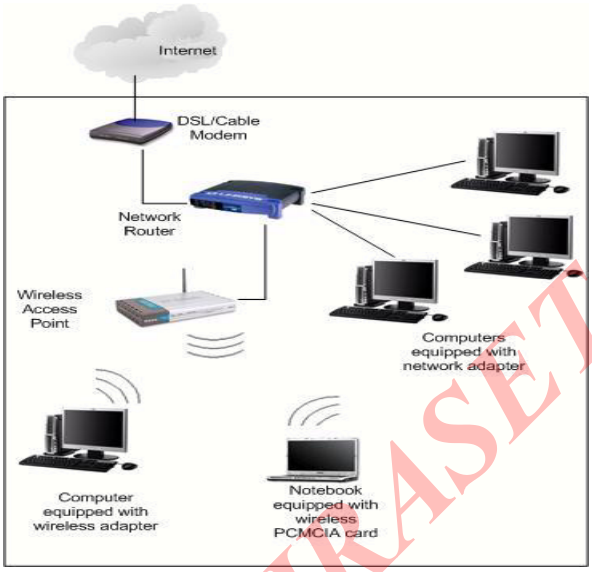

Figure1. Wireless Networks

The idea of a wireless network is sometimes also called an infrastructure-less networking, since the mobile nodes in the network dynamically establish routing among themselves to form their own network on the fly [7]. There are over one billion wireless subscribers today utilizing wireless devices for data services and phone calls. The proliferation of wireless technology, making it possible to extend both data and voice services over the networks and the resulting of anytime, anywhere services make such technologies very attractive to end users.

Characteristics of Wireless Networks

1. Wireless networks are inherently different from well known wired networks. The characteristics of Wireless Networks are as follows:
2. Dynamic changing network topology: The nodes in Wireless Networks are free to move in any direction at any time. So the network topology of the Wireless Networks changes rapidly and randomly at any time.
3. Bandwidth constraints: Wireless links have significantly lower bandwidth than well known wired networks.
4. Energy constraints: Wireless Networks also have nodes whose energy storage is very limited. Often, they are better equipped, with very limited to no recharging or replacement possible.
5. Limited security: Wireless Networks are much more vulnerable to attacks due to their open medium, lack of centralized monitoring, cooperative algorithm and dynamically changing topology.

Node cooperation: Wireless Networks support cooperative algorithms. In Wireless Networks every node is responsible for the routing and forwarding information to maximize the total network throughput.

II.RELETED WORK

A wireless network is one that is an autonomous, self configuring network made up of mobile nodes connected via wireless links. The mobile or portable devices are free to move in any direction and are part of the network only when they are within range. Securing wireless network presents challenges because the nature of wireless networks is highly vulnerable to attacks due to their open medium, lack of centralized policy, dynamic changing topology and cooperative algorithms [8,9].

IN THE YEAR, 2007.

Researchers have found that there is one way of securing a wireless network at the network layer is to secure the routing

IJRASET: ISSN: 2321-9653

protocols such that all the possible attacks are prevented. However, as far as we know, there is no secure routing proposed in literature so far takes care of all kinds of attacks. And if a secure routing protocol would come up, which takes care of all types of attacks, still one can never tell when a different kind of new attack raised and exploits the weakness of the system. The objectives of this chapter are to give an overview of existing secure ad hoc network research.

IN THE YEAR, 2008.

In this paper, they propose a novel approach to flooding, which relies on proactive compensation packets periodically broadcast by every node. The compensation packets are constructed from dropping data packets, based on techniques borrowed from forward error correction. Since our approach does not rely on proactive neighbor discovery and network overlays it is resilient to mobility[10]. They evaluate the implementation of Mistral through simulation and compare its performance and overhead to purely probabilistic flooding.

IN THE YEAR, 2009.

The existing techniques for flooding are not so efficient. So to improve the efficiency of flooding the combination of blind flooding and node caching can be used. In that method cache the nodes which are recently involved in data packet forwarding, and use only them to forward route requests. Dropping route request forwarding from the other nodes considerably reduces routing overhead. After considering the various methods for improving the efficiency of flooding techniques, it is clear that none of them gives an improved solution. Several broadcasting techniques are compared and concluding that neighbor-knowledge based broadcasting is better than probabilistic and area based methods in reducing packet redundancy.

IN THE YEAR, 2010.

This causes high protocol overhead and interference with the existing traffic on the networks. Some efficient flooding algorithms were proposed to avoid these problems. However, these algorithms either perform poorly in reducing redundant transmissions or require each node to maintain 2-hop (or more) neighbors information. In the paper, they studied the sufficient and necessary condition of 100 percent deliverability for flooding schemes that are based on only 1-hop neighbor's information. They further propose an efficient flooding algorithm that achieves the local optimality in two senses: 1) The number of forwarding nodes in each step is minimal and 2) the time complexity for computing forwarding nodes is the lowest, which is O (n log n), where n is the number of neighbors of a node[11].

IN THE YEAR, 2011.

In which Data dissemination is an important service in mobile ad hoc networks (MANETs). The main objective of that paper was to present a dissemination protocol, called locBcast, which utilizes positioning information to obtain efficient dissemination trees with low control overhead. That paper includes an extensive simulation study that compares locBast with selfP, dominantP, fooding, and a couple of probabilistic-/counter-based protocols. It is shown that locBcast behaves similar to or better than those protocols and is especially useful in the following challenging environments: the message sizes are large, the network is dense, and nodes are highly mobile.

IN THE YEAR, 2012.

In which Mobile Ad hoc Network (MANET) is a self-organizing, infrastructure less, multi hop network. The flooding scheme, used to discover routes in MANET is shown to cause high retransmissions, packet collisions and media congestion that can significantly degrade the network performance. Flooding must be handled efficiently in order to improve the performance of the protocol. The existing techniques for flooding are not so efficient. So to improve the efficiency of flooding the combination of blind flooding and node caching can be used. In that method cache the nodes which are recently involved in data packet forwarding, and use only them to forward route requests. Dropping route request forwarding from the other nodes considerably reduces routing overhead

III.PURPOSE of RESEARCH

Research and Application Challenges

The main goal is to design and implement this mechanism that will operate in a wireless network to detect the repeated data packet. We have to implement the packet redundant attacks and an attack in which a node refuses to accept the redundant packet

IJRASET: ISSN: 2321-9653

within a specified interval with AODV routing protocol [12,13]. Finally we need to simulate our proposed algorithm with an appropriate simulator and examine the results to determine the efficiency of the proposed algorithm.

IV. EXPERIMENT and IMPLEMENTATION

We propose an algorithm for Efficient Data Broadcasting in the wireless wireless networks. The node may be defined as a node which does not follow the exact behavior. A node may try to launch the several attacks which were discussed in previous chapters. Most of the attacks are accomplished by modifying a message or simply not to forward the message which it is supposed to forward [14]. While developing the algorithms we used some term and definitions which are discussed in the next sections.

The definitions which are used in our proposed algorithm are as follows:

a. Neighbor: A node that is within wireless transmission range of another node.

b. Transmission Range: The average maximum distance between two nodes in which they seems as the one hop to each other.

c. Neighborhood: All the nodes that are within wireless transmission range of a node.

d. Promiscuous mode: Promiscuous mode can be used to monitor data traffic in a network. If two nodes are in promiscuous mode they can hear transmission from each other [15].

e. wicked node: A wicked node misuses the cooperation among nodes to disturb the operation of the network. A wicked node may try to launch.

f. Route Request Packet (RREQ): This packet is used when a route to the destination is not available. This packet floods in the network by a node to its neighbor with the intension to find the route. This packet always broadcast in the network.

g. Route Reply Packet (RREP): A node that has a fresh route to the destination or the destination itself responds to the request by a route reply (RREP) message. This packet always unicast in the network [16].

h. Data Packet: This packet contains the original data which sender wants to transmit to the receiver.

V.PROPOSED ALGORITHM

A wireless network is most susceptible to flooding attacks. To avoid +being identified, the attackers usually recruit multiple accomplices to dilute attack traffic density of each attack source, and use the address spoofing technique to challenge the attack tracing. We proposed an algorithm which tries to improve the data broadcasting technique for Wireless network [9,17].

Repeat Path Appeal = False

EXISTINGTIME : time on the system clock

ACKNOWLEDGED TIME : the value of acknowledged Time phase of the node

FURTHER TIME : the value of forward Time period for the node

Total No. of Appeal Acknowledged by the node =False

Drop-Data : 0

INPUT: A Path Appeal Data Packet to node

OUTPUT: Efficient Data Transmission on time of a node.

for all path Appeal Data Packets to Existing node do

if the Existing node a source node and neighbor node is not a Target node

then send path Appeal Data Packet for all neighbors

if duplicate Path Appeal = False && Further Timer =False then

message “Appeal Not forward by the node”

Total No. of Appeal Acknowledged by the node = Total No. of Appeal Acknowledged by the node +1

Drop-data = Drop-data+1

else if duplicate Path Appeal = True && Further Timer =False then

message “Appeal Not forward by the node”

Total No. of Appeal Acknowledged by the node = Total No. of Appeal Acknowledged by the node +1

Drop-data = Drop-data+1

else if duplicate Path Appeal = False && Further Timer =True then

message “Appeal forward Successfully”

Total No. of Appeal acknowledged by the node = Total No. of Appeal Acknowledged by the node +1

Drop-data = Drop-data

else

message “reject the replicate path Appeal ”

else

message “Neighbor is a Target node”

end for

IJRASET: ISSN: 2321-9653

VI. RESULT

We discuss about the results of simulation and evaluate the performance of the proposed algorithm. Here, firstly we are discussing about simulation parameters which are shown in table below: [15].

	Simulation Parameters	Values
1	Simulator Used	Network Simulator (version 2.34)
2	Number of Nodes	100
3	No. of nodes	10, 20, 30
4	Routing Protocol	AODV
5	Area Size	1900m×1900m
6	MAC	802.11
7	Simulation Time	200Secs
8	Traffic Source	CBR
9	Speed	10m/s
10	Pause Time	2sec

After the analysis of result we have shown the screenshots are as follows:

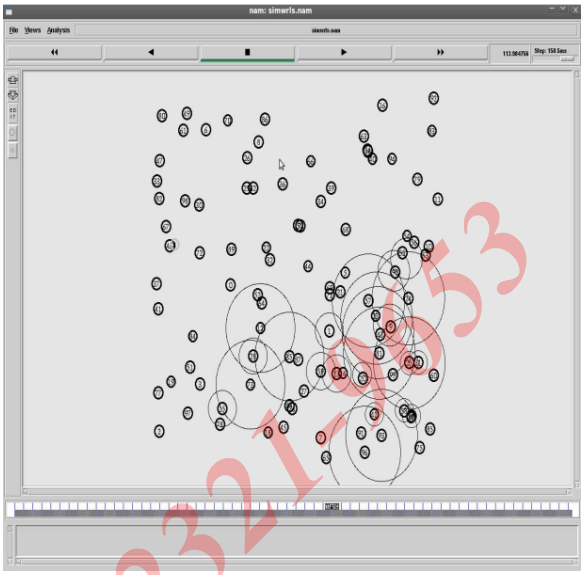

Figure 3: Screenshot 2 of NAM visualization of output

In order to evaluate the performance of the proposed approach we use three measures: Detection Efficiency

Table 5.2: Effectiveness (%)

No. of Nodes	Maximum Connection=10		Maximum Connection=20	
	Threshold(20)	Threshold(30)	Threshold(20)	Threshold (30)
10	89	79	100	89.5
20	74	69	94	82.5
30	72	59	89	81

IJRASET: ISSN: 2321-9653

VII. CONCLUSION

Today wireless technologies are frequently used transversely the world to hold up the communication needs of a huge number of end users. In the presented work, the goal is to improve the efficiency of AODV routing protocol by reducing the flooding in the MANET. Flooding is the by default method of broadcasting. As such, the plain flooding algorithm provokes a high number of unnecessary packet rebroadcasts, causing contention, packet collisions and ultimately wasting precious limited bandwidth. This flooding overhead is reduced by using probabilistic scheme. In this scheme, when receiving a broadcast message for the first time, a node rebroadcasts the message with a pre-determined probability p; every node has the same probability to rebroadcast the message (symmetric environment).The performance of AODV has been measured with respect to metrices viz. control packet overhead, average end to end delay and retransmitting nodes under varying node mobility environment. The results indicate that in high node density the performance of the protocol increases significantly, whenever the network density increases in number of nodes greater than 80 nodes.The reason of performance up gradation is due to the fact when probability increases with increase in the number of nodes the control packet over head, average end to end delay and retransmitting nodes varies with node mobility increases or decreases due to probability approach. In current work, only three performance metrics have been considered to analyze the performance of AODV. [16].

VIII. FUTURE WORK

We will propose an algorithm for Efficient Data Broadcasting in the wireless wireless networks[17]. In the future, we will simulate our proposed algorithm using network simulator version 2 as well as, we would like to extend this scheme to detect other type of attacks such as application layer attack, denial of service, manipulation of network traffic and so on. We can also mount this algorithm with other wireless routing protocols such as DSR, TORA and with other types of attacks

REFERENCES

[1] Ningrinla Marchang and Raja Datta. "Collaborative techniques for intrusion detection in mobile ad-hoc networks",*Ad Hoc Networks*, 6(4): pp 508–523, 2008.

[2] Farooq Anjum and Petros Mouchtaris. "Security for Wireless Ad Hoc Networks" . WILEY, 2nd edition, 2007.

[3] Yu-Chee Tseng, Sze-Yao Ni and En-Yu Shih "Adaptive Approaches to Relieving Broadcast Storms in a Wireless Multihop Mobile Ad Hoc Network", IEEE TRANSACTIONS ON COMPUTERS, VOL. 52, NO. 5, Pp: 554-557, MAY 2003

[4] J Yick, B Mukherjee… -"Computer networks", 2008 – Elsevier

[5] Yu-Chee Tseng, Sze-Yao Ni, Yuh-Shyan Chen and Jang-Ping Sheu "The Broadcast Storm Problem in a Mobile Ad Hoc Network", Wireless Networks 8, 153–167, 2002, Kluwer Academic Publishers.

[6] Yongguang Zhang and Wenke Lee. "Intrusion detection in wireless ad-hoc networks". In *MOBICOM*, pp 275–283, 2000.

[7] William Stallings."Cryptography and Network Security principles and practices". Pearson Education Inc, third edition, 2003.

[8] Joseph P. Macker, Justin Dean and William Chao "Simplified Multicast Forwarding in Mobile Ad hoc Networks".Military Communications Conference, 2004. MILCOM 2004. 2004 IEEE (Volume:2).Pp: 744-750.

[9] Wei Peng and Xi-Cheng, "On the Reduction of Broadcast Redundancy in Mobile Ad Hoc Networks", IEEE,2000.

[10] Christine e. Jones, Krishna m. Sivalingam, prathima agrawal and jyh cheng chen "A Survey of Energy Efficient Network Protocols for Wireless Networks", Wireless Networks 7, 343–358, 2001, Kluwer Academic Publishers.

[11] PENG Wei and LU Xicheng "an efficient Broadcast Protocol for Mobile Ad Hoc Networks", Vol.16 No.2 J. Computer Science & Technology, Mar. 2001.

[12] Mobile ad hoc network. http ://en:wikipedia:org/wiki/Mobile_ad_hoc_network.

[13] Wenrui Zhao, Mostafa Ammar and Ellen Zegura proposed A Message Ferrying Approach for Data Delivery in Sparse Mobile Ad Hoc Networks, MobiHoc'04, May 24–26, 2004, Roppongi, Japan.

[14] Stefan Pleisch, Mahesh Balakrishnan, Ken Birman and Robbert van Renesse developed MISTRAL: Efficient Flooding in Mobile Adhoc Networks, MobiHoc'06, May 22–25, 2006, Florence, Italy.

[15] Hai Liu, Xiaohua Jia, Peng-Jun Wan, Xinxin Liu, and Frances F. Yao "A Distributed and efficient Flooding Scheme using 1-Hop Information in Mobile Ad Hoc

IJRASET: ISSN: 2321-9653

Networks" .IEEE transactions on parallel and distributed systems, vol. 18, no. 5, may 2007.

[16] Adnan Agbaria, Muhamad Hugerat and Roy Friedman "Efficient and Reliable Dissemination in Mobile Ad Hoc Networks by Location Extrapolation", Hindawi Publishing Corporation, Journal of Computer Networks and Communications, Volume 2011, Article ID 680936, 11 pages.

[17] Chaithannia T S and Ashly Thomas T "Different Enhancements for Flooding Scheme in Mobile Ad hoc Networks", Conference on Advances in Computational Techniques (CACT) 2011 Proceedings published in International Journal of Computer Applications, Pp : 10-13.

IJRASET: ISSN: 2321-9653