Collision Detection in MANET based on Network Coding Technique

J. Srinivasan [#1], S. Sudha [*2]

[#] Assistant Professor,CSA Department, SCSVMV University, Kanchipuram, TN, India.

[1] vsrini082@gmail.com

[*] PG Scholar, Dept. of CSE, RRase Engineering College, Padappai, TN, India.

Abstract*- In the recent years, the wireless mobile ad-hoc network (MANET) plays a significant role in numerous fields in very effective manner such that fields like battlefields, industrial applications, signal routing traffic surveillance and so on. This type of the wireless networks is an increasing emerging technology nowadays and having the great impending to apply in the serious situations. The wireless mobile ad-hoc networks is emerging technology has been protected by various systems such as firewall's, Antivirus, and so on. Though MANET has many securities policy to protect the privacy in the communication, the adversaries easily interfere in the mobile ad hoc networks and collapse all the data's or information. The MANET is not having any infrastructure or any centralized server to control entire networks. A devices is connected in the MANET is independent to move anywhere and change the connection to the other devices frequently and the device connected in the MANET is mobility in nature. Due to the various changes in the devices communication, security level in the open environment is low when compared to the centralised server using networks. So the various types of attacks are easily happen in the MANET. The existing systems are not sufficient and effective in preventing the attacks or collision of nodes in the entire mobile networks. So the MANET required some effective method to monitors the networks defects, misbehaving nodes, and collision nodes and also to prevent the attacks from attackers. And the other case in this paper is intermediates Nodes swap over the information if the nodes at a reserve at mainly contained by both, wherever is the node communication radius in the mobile ad hoc networks. The flooding time of the mobile nodes is the quantity of time-steps essential to transmit a message from client node to each and every node of the entire network. Flooding time is very significant for to analysis of how quickly information or data can broaden in the entire mobile ad hoc networks In the existing system the problem of Privacy threat is not handled and so we extend our work by proposing an efficient system of local broadcasting with security enhancement. In this paper, We recognize that Privacy risk in the MANET is one of the serious obstacles in multihop wireless networks. This type of privacy attacks or obstacles collapse the traffic analysis of data and dataflow tracing can be easily launched by a malicious adversary due to the open wireless medium of the networks. In order to overcome the above issues in the mobile ad hoc networks, we proposed the effective method of network coding Technique. Our proposed technique in this paper has more efficient than the other methods. Our experimental analysis show that the effectiveness of our proposed method as following in the paper.

Index Terms*- Mobile ad-hoc network (MANET), Security, algorithms, and collision of nodes, flooding time of data, intrusion detection system (IDS), attacks, privacy threat.

I. INTRODUCTION

In the next generation of wireless communication systems [1], there will be a need for the rapid deployment of independent mobile users. Significant examples include establishing survivable, efficient, dynamic communication for emergency/rescue operations, disaster relief efforts, and military networks. Such network scenarios cannot rely on centralized and organized connectivity, and can be conceived as applications of Mobile Ad Hoc Networks. A MANET is an autonomous collection of mobile users that communicate over relatively bandwidth constrained wireless links. Since the nodes are mobile, the network topology may change rapidly and unpredictably over time. The network is decentralized, where all network activity including discovering the topology and delivering messages must be executed by the nodes it, i.e., routing functionality will be incorporated into mobile nodes.

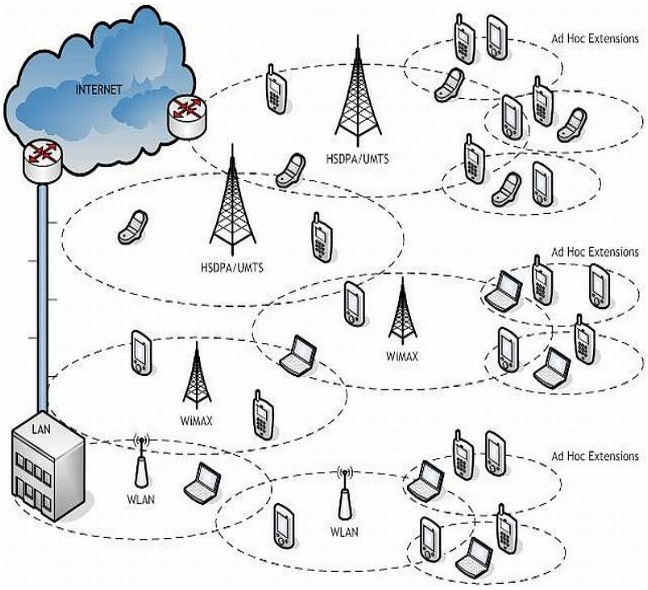

Figure 1- Architecture of Mobile Ad hoc Networks

Wireless ad-hoc networks [12] play a vital role in the communications fields. This is due to the strong signal transmission at the critical situation also in the battle fields. These type of wireless communication also used for the various purposes. Wireless mobile Ad-hoc network (MANET) and its various attacks and also discuss about the collision of the nodes in the networks. The MANET is attacked by different types of attacks but the collision of nodes occurs due to mobility of the mobile and deals with the flooding time of the networks, whereas the communication between the two or more devices by intermediate nodes itself without any centralized system so that attacks can be achieved easily in the network. The flooding time is very significant role in the mobile ad hoc networks.

The existing systems are not sufficient and effective in preventing the attacks or collision of nodes in the entire mobile networks. So the MANET required some effective method to monitors the networks defects, misbehaving nodes, and collision nodes and also to prevent the attacks from attackers. And the other case in this paper is intermediates Nodes swap over the information if the nodes at a reserve at mainly contained by both, wherever is the node communication radius in the mobile ad hoc networks. The flooding time of the mobile nodes is the quantity of time-steps essential to transmit a message from client node to each and every node of the entire network. Flooding time is very significant for to analysis of how quickly information or data can broaden in the entire mobile ad hoc networks In the existing system the problem of Privacy threat is not handled and so we extend our work by proposing an efficient system of local broadcasting with security enhancement. In this paper, We recognize that Privacy risk in the MANET is one of the serious obstacles in multihop wireless networks. This type of privacy attacks or obstacles collapse the traffic analysis of data and dataflow tracing can be easily launched by a malicious adversary due to the open wireless medium of the networks. In order to overcome the above issues in the mobile ad hoc networks, we proposed the effective method of network coding Technique. Our proposed technique in this paper has more efficient than the other methods. Using our proposed technique, we also analysis the energy efficient of the entire mobile ad hoc networks.

Some of the remaining parts of the paper will see in the following sections. In section 2, we see about the related works of the Mobile ad hoc networks. In section 3, we discuss about our proposed method of network coding technique for energy efficient for local broadcast and secure for the privacy threat. The algorithms and simulation are shown in the section 4 and 5. The conclusion of our paper is in section 6.

II. Related Works

In this section, we will see the some of the related works to the intrusion detection system using different approaches:

Abraham Yaar, Adrian Perrig and Dawn Song[2], proposes a scheme of a path identification mechanism against the DDOS attacks by introducing the PI(path identifier). Distributed Denial of Service (DDOS) attacks continue to plague the Internet. Defense against these attacks is complicated by spoofed source IP addresses, which make it difficult to determine a packet's true origin. We propose Pi (short for Path Identifier), a new packet marking approach in which a path fingerprint is embedded in each packet, enabling a victim to identify packets traversing the same paths through the Internet on a per packet basis, regardless of source IP address spoofing.

Jelena Mirkovic, Janice Martin and Peter Reihe[3], This paper proposes a taxonomy of distributed denial-of service attacks and a taxonomy of the defense mechanisms that strive to counter these attacks. The attack taxonomy is illustrated using both known and potential attack mechanisms. Along with this classification we discuss important features of each attack category that in turn define the challenges involved in combating these threats. The defense system taxonomy is illustrated using only the currently known approaches. The goal of the paper is to impose some order into the multitude of existing attack and defense mechanisms that would lead to a better understanding of challenges in the distributed denial-of-service field.

Li-chiou chen and Kathleen M Carley [4] proposes a method to defense against the DDOS attack on website by developing the computational testbed and its associated technology.

Sanjay B Ankali and Dr. D V Ashoka [5] proposed a scheme to prevent the internet from the DDOS attacks by using the HTTP and FTP architecture. This paper designs two independent architectures for HTTP and FTP which uses an extended hidden semi-Markov model is proposed to describe the browsing habits of web searchers.

Prachi Bansal, Beenu Yadav, Sonika Gill, Harsh Verma [6], Wireless Sensor Networks (WSNs) use small nodes with constrained capabilities to sense, collect, and disseminate information in many types of applications. One of the major challenges wireless sensor networks face today is security Wireless Sensor Networks (WSN) is an emerging technology and have great potential to be employed in critical situations like battlefields and commercial applications such as building, traffic surveillance, habitat monitoring and smart homes and many more scenarios. One of the major challenges wireless sensor networks face today is security. In this paper we present a introduction to wireless sensor networks, its usage in every environment followed by a brief overview of characteristics and requirements for deploying such a network. The different attacks on these networks are discussed. For each of these attacks, counter measures are presented if applicable.

S. G. Shiva Prasad Yadav , Dr. A. Chitra [7], In this technical paper a survey on recent trends in wireless sensor network research, different topologies, routing protocols, simulators and applications is carried out. A smart WSN consists of sensor nodes made of small electronic device and are deployed across a geographical area. These nodes carry out the sensing, processing and transmission of data from different physical environments. They depend on batteries which get drained very soon due to the computation and data transmission to other nodes. The architectures of WSN are mainly depending on application requirements.

WSN is a multidisciplinary area of research where different applications developers, users, hardware and software designers need to work closely to implement an efficient application. The different characteristics of the sensor network like flexibility, fault tolerance, high sensing fidelity, low cost and rapid deployment create many new and exciting application areas.

Ashraf Darwish and Aboul Ella Hassanien [8], Wireless sensor network (WSN) technologies are considered one of the key research areas in computer science and the healthcare application industries for improving the quality of life. The purpose of this paper is to provide a snapshot of current developments and future direction of research on wearable and implantable body area network systems for continuous monitoring of patients. This paper explains the important role of body sensor networks in medicine to minimize the need for caregivers and help the chronically ill and elderly people live an independent life, besides providing people with quality care. The paper provides several examples of state of the art technology together with the design considerations like unobtrusiveness, scalability, energy efficiency, security and also provides a comprehensive analysis of the various benefits and drawbacks of these systems. Although offering significant benefits, the field of wearable and implantable body sensor networks still faces major challenges and open research problems which are investigated and covered, along with some proposed solutions, in this paper.

Sanjay P. Ahuja, and Jack R. Myers [9], this paper presents a survey of the current state of wireless grid computing. This includes a discussion of the cooperation between wired and wireless grids including ways in which wireless grids extend the capabilities of existing wired grids. It also discusses many of the new capabilities and resources available to wireless grid devices and a sampling of several applications of these new resources. It provides a sampling of many current research endeavors in the wireless grid arena and an examination of a number of the potential challenges resulting from the unique characteristics of wireless grid devices.

Norman A. Benjamin and Suresh Sankaranarayanan [10], Wireless sensor network (WSN) has become a significant technology and Wireless (body) sensors can be deployed on patients to continually monitor their physiological health conditions. The wireless body sensors can then be configured to convey the patient's status directly to the assigned doctor/nurse through the personal smart phone, PDA or Palm device. In this situation, Wireless Mesh Networks (WMN) can be used to transmit vital information arising from the wireless Body sensor Network (WBSN) to the backbone network. It may be mentioned that WMN which is an extension of LAN, has far better range involving very little wiring. The integration of WBSN and WMN technologies, results in Wireless Sensor Mesh Network (WSMN) and this technique has already been proposed by one of the authors of this paper, for usage in the medical field. In this paper we present the results on the performance of such a WSMN used for patient health monitoring application, in terms of parameters like delay, MAC delay and throughput under varying number of patients and varying number of doctors in wards and also the failure performance when the mesh nodes fail based on simulation study carried out.

III. Proposed Work

In this paper, we mainly discuss about wireless mobile Ad-hoc network (MANET) and its various attacks and also discuss about the collision of the nodes in the networks. The MANET is attacked by different types of attacks but the collision of nodes occurs due to mobilitiness of the mobile and deals with the flooding time of the networks, whereas the communication between the two or more devices by intermediate nodes itself without any centralized system so that attacks can be achieved easily in the network. The flooding time is very significant role in the mobile ad hoc networks.

The existing systems are not sufficient and effective in preventing the attacks or collision of nodes in the entire mobile networks. So the MANET required some effective method to monitors the networks defects, misbehaving nodes, and collision nodes and also to prevent the attacks from attackers. And the other case in this paper is intermediates Nodes swap over the information if the nodes at a reserve at mainly contained by both, wherever is the node communication radius in the mobile ad hoc networks. The flooding time of the mobile nodes is the quantity of time-steps essential to transmit a message from client node to each and every node of the entire network. Flooding time is very significant for to analysis of how quickly information or data can broaden in the entire mobile ad hoc networks In the existing system the problem of Privacy threat is not handled and so we extend our work by proposing an efficient system of local broadcasting with security enhancement. In this paper, we recognize that Privacy risk in the MANET is one of the serious obstacles in multihop wireless networks. This type of privacy attacks or obstacles collapse the traffic analysis of data and dataflow tracing can be easily launched by a malicious adversary due to the open wireless medium of the networks. In order to overcome the above issues in the mobile ad hoc networks, we proposed the effective method of network coding Technique. In order to reduce the nodes collision and efficient low energy consumption for the local data or information broadcast between the intermediate nodes present in the mobile ad hoc networks. So we suggest our effective model of local broadcast algorithm with Network Coding Technique. Network coding has the latent to frustrate the privacy attacks from the adversaries because the coding/integration process is expectant at intermediary nodes. Our proposed technique in this paper has more efficient than the other methods. Using our proposed technique, we also analysis the energy efficient of the entire mobile ad hoc networks.

IV. ALGORITHM

```
start Broadcast, vigil node;
mark unique node id;
stamp the message with source id;
if (message is new)
forward it;
else
discard message;
end if
maintain a list of  nodes through which the message passed;
if(collision found)
stop forwarding messages;
empty the queue;
end if;
end;
```

V. RESULT ANALYSIS

We have simulated our system in NS2. We implemented and tested with a system configuration on Intel Dual Core processor, Windows XP and using CYGWIN. We have used the following modules in our implementation part. The results for this system are as follows:

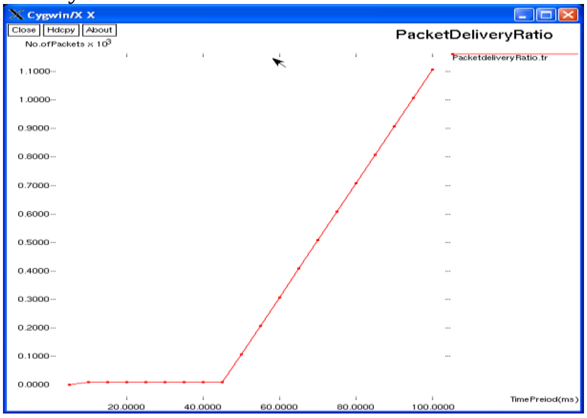

Figure 2- Packet Delivery Ration

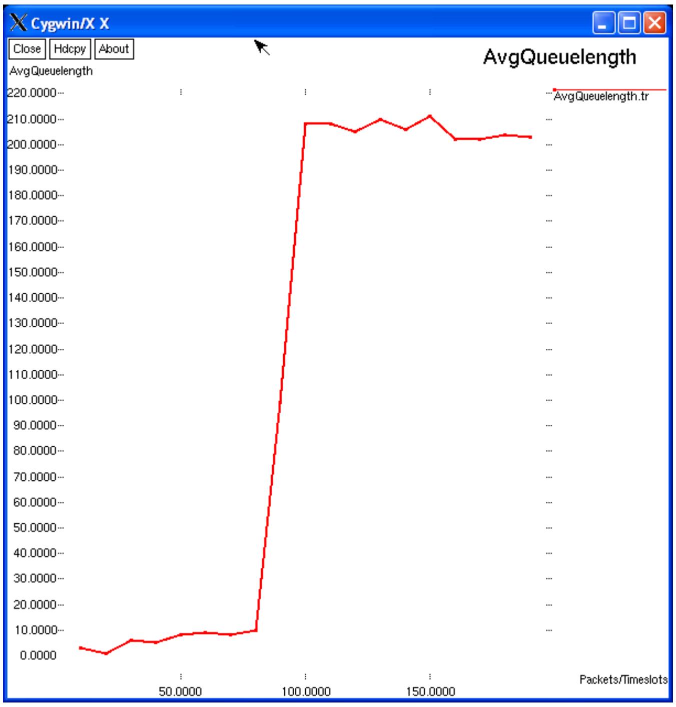

Figure 3- Average Queue Length

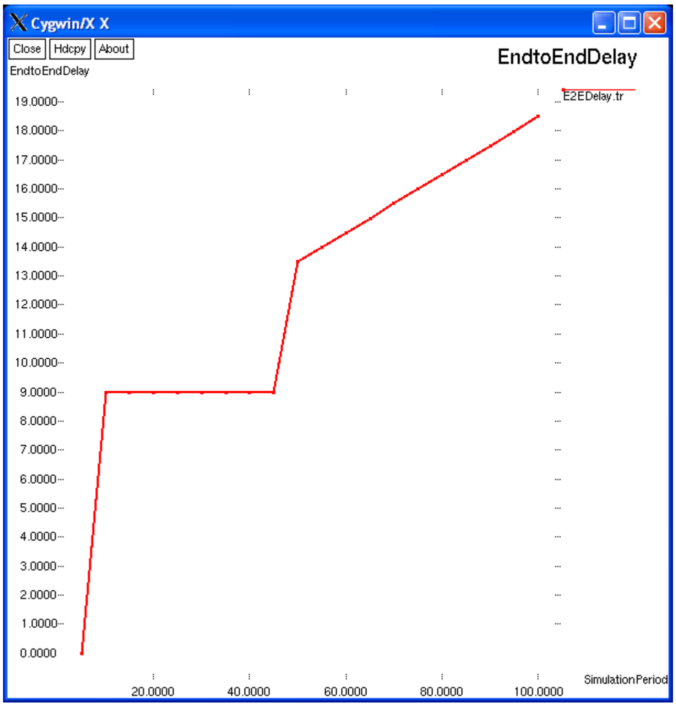

Figure 4- End – to – End Delay

VI. Conclusion

Our proposed network coding techniques in this paper destroys the need of centralised control and security level issues for the connectivity of the nodes. Our experimental results exhibited the effective to reduce the collisions of mobile nodes in the networks. In order to reduce the nodes collision and efficient low energy consumption for the local data or information broadcast between the intermediate nodes present in the mobile ad hoc networks. So we suggest our effective model of local broadcast algorithm with Network Coding Technique. Network coding has the latent to frustrate the privacy attacks from the adversaries because the coding/integration process is expectant at intermediary nodes. Our proposed technique is also applied for the securing purposes for other wireless networks. Our experimental result showed that our technique works efficiently when compared to previous methods.

VII. References

[1] [Definition from the link: http://w3.antd.nist.gov/wahn_mahn.shtml

[2] Abraham Yaar Adrian Perrig Dawn Song Carnegie Mellon University fayaar, perrig, dawnsongg@cmu.edu Pi: A Path Identification Mechanism to Defend against DDoS Attacks

[3] Jelena Mirkovic, Janice Martin and Peter Reiher A Taxonomy of DDoS Attacks and DDoS Defense Mechanisms Computer Science Department University of California, Los Angeles Technical report #020018

[4] Li-chiou chen and Kathleen M Carley Modelling Distributed Denial Of Service Attacks and Defenses

[5] Sanjay B Ankali Department of Information Science & Engg, SJBIT, Bangalore, India Email: sanjay.ankali@yahoo.com Dr. D V Ashoka, Professor & Head, Department of Information Science & Engg, SJBIT, Bangalore, India Email: dr.ashok_research@hotmail.com Detection Architecture of Application Layer DDoS Attack for Internet Int. J. Advanced Networking and Applications Volume: 03, Issue: 01, Pages:984-990 (2011)

[6] Prachi Bansal, Beenu Yadav, Sonika Gill, Harsh Verma “Security Attacks in Wireless Sensor Network”- International Journal of Scientific & Engineering Research, Volume 3, Issue 4, April-2012 1ISSN 2229-5518.

[7] S. G. Shiva Prasad Yadav , Dr. A. Chitra “Wireless Sensor Networks - Architectures, Protocols, Simulators and Applications: a Survey”- International Journal of Electronics and Computer Science Engineering.

[8] Ashraf Darwish and Aboul Ella Hassanien “Wearable and Implantable Wireless Sensor Network Solutions for Healthcare Monitoring”- Received: 3 April 2011; in revised form: 14 May 2011 / Accepted: 19 May 2011 / Published: 26 May 2011

[9] Sanjay P. Ahuja, and Jack R. Myers “A Survey on Wireless Grid Computing”- July 2006, Volume 37, Issue 1, pp 3-21

[10] Norman A. Benjamin and Suresh Sankaranarayanan “Performance of Wireless Body Sensor based Mesh Network for Health Application”- International Journal of Computer Information Systems and Industrial Management Applications (IJCISIM).

[11] Prajeet Sharma, Niresh Sharma and Rajdeep Singh “A Secure Intrusion detection system against DDOS attack in Wireless Mobile Ad-hoc Network”- International Journal of Computer Applications (0975 – 8887) Volume 41– No.21, March 2012

[12] B. Sri Lakshmi, N. Pavani and K.V. Narasimha Reddy “On Probe Packet Based Intrusion Detection System”- INTERNATIONAL JOURNAL OF EMERGING TECHNOLOGY IN COMPUTER SCIENCE AND ELECTRONICS (IJETCSE) – VOLUME 1 ISSUE 1 – AUGUST 2013.