Simulation and Analysis of Attacks and Quality of Service (QoS) in Cyberspace

M.Dervin Moses [1], **M.Rajha** [2]

[1,2] *P.G.Student, Information and Technology, Francis Xavier Engg., College,Tirunelvelli, Tamilnadu, India*

Abstract - *Now a days, Botnets have major engines for malicious attacks in wireless communication fields. It is very hard for botnet owners to satisfy the condition to carry out attack most of the time. This poses a critical challenge in anomaly detection So, the necessity security methods is most important to check the Quality of Service of packet transmission without any threads. In this paper, we use wireless sensor network based data transmission system for detection of different attacks and check whether they reached the successful transmission of packet transmission in cyberspace. The quality of QoS (Quality of service Oriented Distributed routing protocol) is improved and a protocol named EQOD (Enhanced Quality of service Oriented Distributed routing protocol) is developed. The EQOD protocol improves the throughput and decreases the overhead in the network and avoids the energy harvesting problem. Hence the results are proved that the improved QOS and high security.*

Key Words: Wireless Network1, Quality of Service2, Security3, and EQOD4.

1. INTRODUCTION

As wireless communication gains popularity, significant research has been devoted to support real time transmission with stringent quality of service requirements for wireless applications. At the same time, a wireless hybrid network that integrates a mobile wireless ad-hoc network and a wireless infrastructure network has been proven to be a better alternative for the next generation wireless network. Quality of service Oriented Distributed routing protocol enhances the quality of service capability of hybrid networks.Wireless Sensor Network mechanism is quite simple and applicable to a variety of fields. It is based on nodes, controllers, radio transceivers and batteries. The key to stimulate the sensor networking is the algorithm sponsor multi-router phenomenon. The system is totally dependent on the nodes and the harmony established between them through proper frequency. These nodes are of different sizes according to the function they perform[1].

To activate the monitoring or tracking function of these nodes, a radio transmitter is attached to forward the information. They are controlled by the microcontroller according to the function. All the systems are in working condition with the help of energy supply which is in the form of battery. The wireless sensor networks perform function concurrently where the nodes are autonomous bodies incorporated in the field spatially for the accurate results[2]. The information transmits through proper channel taking the information collecting it in the form of data and send to the base. Infrastructure networks in WSN contain special nodes called access points (APs), which are connected via existing networks. APs are special in the sense that they can interact with wireless nodes as well as with the existing wired network. The other wireless nodes, also known as mobile stations (STAs), communicate via APs. The APs also act as bridges with other networks.

1.1 Hybrid Network

Fig 1. shows the different types of protocols. Mainly the hybrid network consists of various base stations within the various coverage areas. All the base stations in different coverage areas are connected together for transmitting the datas from the source to the destination through various intermediate nodes. The first approaches were aimed at mobile ad hoc networks and enforced co-operation by threat of punishment. In the Nuglet scheme, a node can only transmit self-generated packets when it has forwarded enough packets from its neighbors before. In the Confidant approach, the behavior of a node is monitored by its neighbors and a selfish node will be isolated from the network. In both concepts a node can be excluded from participating in the network without itself being at fault (starvation or collective false accusation). With the Sprite scheme, rewards have been introduced as incentive for cooperation in mobile ad hoc networks. Nodes report their forwarding activities to a central authority reachable via an overlay network. In conjunction with the missing security mechanisms, this scheme seems highly vulnerable to attacks and transmission errors. In this suggest the usage of rewards in multi-hop cellular networks and let a central authority collect and analyze reports to decide about rewards and punishments.

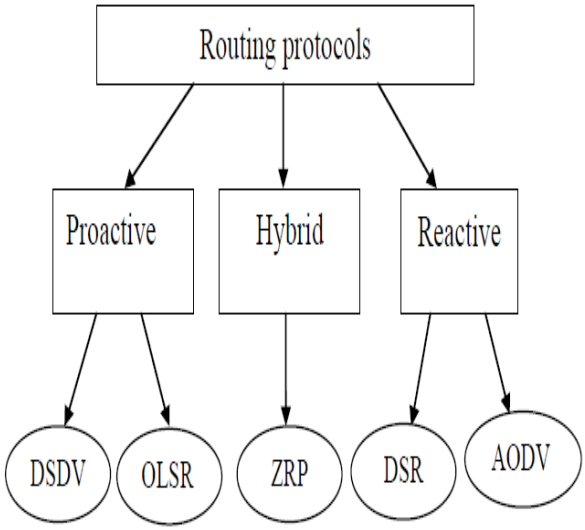

Fig-1: Types of Protocols

2. LITERAURE SURVEY

In this paper [3], a new intrusion-detection system named Enhanced Adaptive ACKnowledgment (EAACK) is proposed and it is specially designed for MANETs. However, the open medium and wide distribution of nodes make MANET vulnerable to malicious attackers. In this case, it is crucial to develop efficient intrusion-detection mechanisms to protect MANET from attacks. In this paper [4], a QoS-Oriented Distributed routing protocol (QOD) to enhance the QoS support capability of hybrid networks is proposed. Taking advantage of fewer transmission hops and any cast transmission features of the hybrid networks, QOD transforms the packet routing problem to a resource scheduling problem. QOD incorporates five algorithms. In this paper [5], consider finite-state Markov channels in the relay-selection problem. Moreover, this also incorporate adaptive modulation and coding, as well as residual relay energy in the relay-selection process. The objectives of the proposed scheme are to increase spectral efficiency, mitigate error propagation, and maximize the network lifetime. In this paper [6], the weakness of Watchdog is overcome by the introduction of intrusion detection system called Ex-Watchdog. The main feature of the proposed system is its ability to discover malicious nodes which can partition the network by falsely reporting other nodes as misbehaving and the proceeds to protect the network. Simulation results show that the system decreases the overhead greatly, though it does not increase the throughput. In this paper [7], a survey of common Denial-of-Service (DoS) attacks on
network layer namely Wormhole attack, Black hole attack and Gray hole attack which are serious threats for MANETs is presented. We will also discuss some proposed solutions to detect and prevent these attacks. As MANETs are widely used in many vital applications, lots of research work has to be done to find efficient solutions against these DoS attacks that can work for different routing protocols.

3. PROPOSED METHOD AND RESULTS

Quality-of-Service is a set of service requirements to be met by the network while transporting a flow. Here, a flow is a packet stream from source to a destination (unicast or multicast) with an associated Quality of Service (QoS). In other words, QoS is a measurable level of service delivered to network users, which can be characterized by packet loss probability available bandwidth, end-to end delay, etc. Such QoS can be provided by network service providers in terms of some agreement (Service Level Agreement, or SLA) between network users and service providers. Fig.2 and 3 flow chart show the flow diagram of the proposed technique simulation process. In this, first have to initialize the variables. Then, create the objects for Network simulator, trace analysis and network animator window. Select a particular topology for the configuration. Then create each node and check whether each node is configured .If it is yes then it goes to the connection establishment, otherwise goes to the initialized state. Then, check whether the connection is established or not. If there have no connection established, then terminate the connection. If yes then set the procedure and run the NS2 file. The detection algorithm and simulation output shown in Fig.4.The proposed algorithm follows,

1. Develop the profile of ***P(t)*** for a 24 hours period;
2. Mapping done by the variation of flow fine corren-tropy of page request flows against ***P(t)*** and denote as $W_f(t)$;
3. while {true} do

    Check whether the data send correctly denote as $P'(t)$;

    while {$P1(t) >= P(t)$} do

    a. Following statistical methodology, sample request flows for sufficient sample points;

    b. Calculate the flow fine correntropy $W'(t)$;
    c. Conditions ……

    d. Found attack

    else

    do nothing

    end

    end

end

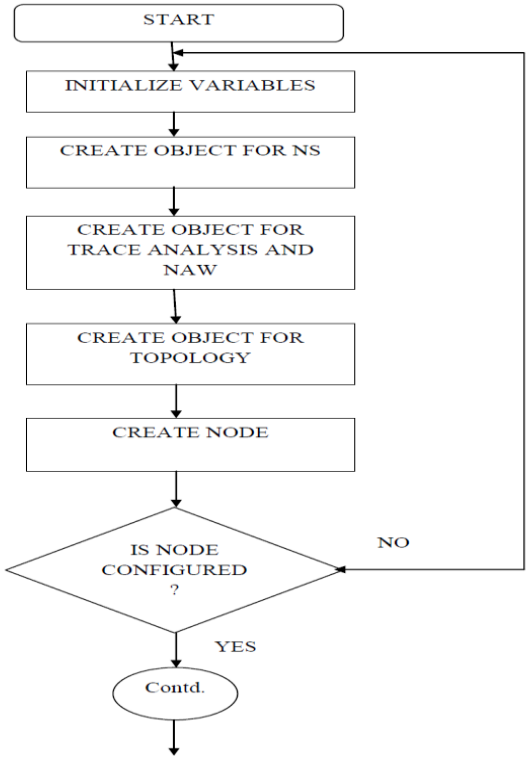

Fig-2.Proposed Technique Flow chart

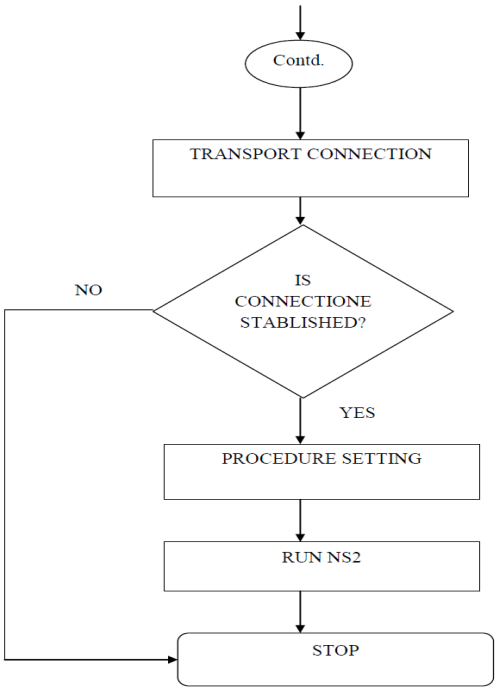

Fig-3. Simulation process

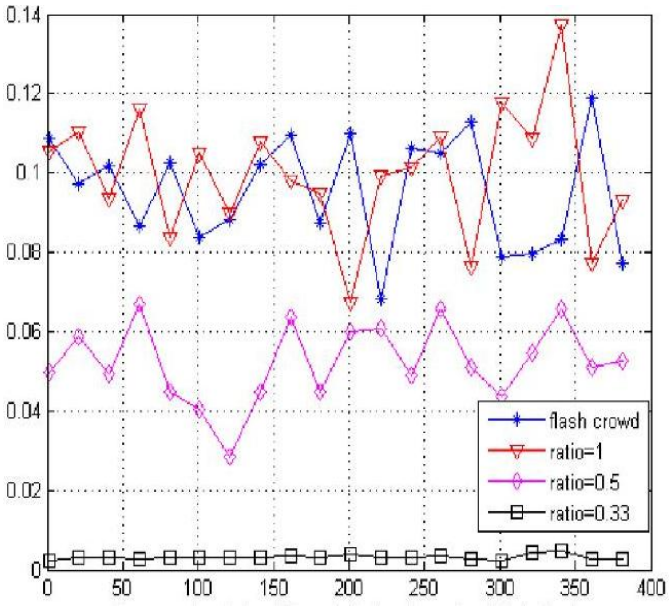

Fig.4 Simulation Output

4. CONCLUSIONS

This paper attempts to improve the quality of QoS protocol in terms of secure data transmission and Packet Delivery Ratio in wireless sensor networks. The proposed techniques are effectively detects and separates the malicious nodes presented in the wireless network with the implementation of the three modes namely the ACK,SACK and MRA modes of the EQOD protocol (Enhanced Quality of service Oriented Distributed routing protocol) . Hence, the obtained results are proved that an effective network with increased Packet Delivery Ratio, decreased transmission delay and high security has been developed.

REFERENCES

[1] AnandPatwardhan, Jim Parker and Anupam Joshi, „Secure Routing and Intrusion Detectionin Ad Hoc Networks‟.Proceedings of the 3rd IEEE Int‟l Conf. on Pervasive Computing and Communications (PerCom 2005).

[2] C. Shen and S. Rajagopalan, „Protocol-independent multicast packet delivery improvement service for mobile ad hoc networks‟.Ad Hoc Networks,2007.

[3] Elhadi M. Shakshuki, Nan Kang and Tarek R. Sheltami, „EAACK-A Secure Intrusion-Detection System for MANETs‟. IEEE TRANSACTIONS ON INDUSTRIAL ELECTRONICS, VOL. 60, NO. 3, MARCH 2013M.

[4] Z. Li and H. Shen,„ A QoS-oriented distributed routing protocol for hybrid networks‟. In Proceedings of MASS, 2010.

[5] Y. Wei, M. Song, F. R. Yu, Y. Zhang, and J. Song, „Distributed optimal relay selection for QoS

provisioning in wireless multi-hop cooperative networks". In Proceedings of GLOBECOM, 2009.

[6] Nidal Nasser and Yunfeng Chen, „Enhanced Intrusion Detection System for Discovering Malicious Nodes in Mobile Ad hoc Networks". IEEE Communications Society, publication in the ICC 2007 proceedings.

[7] Rutvij H. Jhaveri, Sankita J. Patel and Devesh C. Jinwala, „DoS Attacks in Mobile Ad-hoc Networks: A Survey".International Conference on Advanced Computing & Communication Technologies, 2012.

